

绿盟网络入侵防护系统

用户使用手册

文档版本：**V5.6.3.25-20090828**



目录

插图索引

前言

文档范围

本文将覆盖绿盟网络入侵防护系统（NSFOCUS Network Intrusion Prevention System，以下简称 NSFOCUS NIPS）的 Web 管理界面和串口管理界面的所有功能点，详细介绍使用方法。

期望读者

期望了解本产品主要技术特性和使用方法的用户、系统管理员、网络管理员等。本文假设您对下面的知识有一定的了解：

- 系统管理
- Linux 和 Windows 操作系统
- TCP/IP 协议

内容简介

一、产品概述：NSFOCUS NIPS 的简单介绍。

二、基础知识：介绍 NSFOCUS NIPS 基本的使用知识（涉及到功能线索、概念和原理），阅读本章对理解产品的整体功能结构有很大帮助。

三、登录引擎 Web 管理界面：介绍登录 NSFOCUS NIPS 的 Web 管理界面、导入证书和确认系统状态的方法。

四、部署方式：详细介绍 NSFOCUS NIPS 的几种典型部署方式。

五、策略配置：详细介绍 NSFOCUS NIPS 的策略配置方法。

六、查看实时事件：介绍 NSFOCUS NIPS 的实时事件查看方法。

七、日志分析：介绍 NSFOCUS NIPS 的日志查看方法。

八、统计报表：介绍 NSFOCUS NIPS 的报表查看方法。

九、系统维护：介绍常用的系统维护方法。

十、引擎串口配置：详细介绍 NSFOCUS NIPS 串口管理界面的登录方法和使用方法。

十一、NSFOCUS NIPS 规则库：介绍 NSFOCUS NIPS 规则库的使用方法。

附录：NSFOCUS NIPS 引擎（硬件）和安全中心的出厂默认配置，以及串口通讯参数。

获得帮助

如需获取网络安全相关资料，请访问绿盟科技网站：http://www.nsfocus.com

如需获取更详尽的绿盟科技网络安全专业服务信息、商务信息，您可通过如下方式与我们联系：

客户服务热线：400-818-6868（手机和固话均可拨打）

非工作时间服务热线：13321167330

网站：http://support.nsfocus.com

Email：support@nsfocus.com

格式约定

粗体字 —— 命令和关键字

斜体字 —— 需要您输入的变量

—— 使用技巧、建议和引用信息等

—— 重要信息

【XXX】—— 菜单名称和按钮名称的表示方式

【A】➔【B】—— 菜单项选择的表示方式

注：本文中所有图例均为屏幕截取。

一. 产品概述

近年来，企业所面临的安全问题越来越复杂，安全威胁正在飞速增长，尤其混合威胁的风险，如蠕虫、病毒、间谍软件、DDoS 攻击、垃圾邮件、网络资源滥用（P2P 下载、IM 即时通讯、网游、视频……）等，极大地困扰着用户，给企业的信息网络造成严重的破坏。

绿盟网络入侵防护系统（NSFOCUS NIPS）是绿盟科技自主知识产权的新一代安全产品，作为一种在线部署的产品，其设计目标旨在准确监测网络异常流量，自动对各类攻击性的流量，尤其是应用层的威胁进行实时阻断，而不是在监测到恶意流量的同时或之后才发出告警。这类产品弥补了防火墙、入侵检测等产品的不足，提供动态的、深度的、主动的安全防御，为企业提供了一个全新的入侵防护解决方案。

绿盟网络入侵防护系统采用先进的体系架构集成领先的入侵防护技术，包括以全面深入的协议分析技术为基础，协议识别、协议异常检测、关联分析为核心的新一代入侵防护引擎，能够协助客户：

◆ **网络防护**

NSFOCUS NIPS 具有实时的、主动的网络防护功能，内置基于状态检测的防火墙，保护网络边界和内部网络，同时为网络设备的漏洞提供防护，具有流量管理功能，对于可能出现的异常流量，提供抗拒绝服务攻击功能。

◆ **应用防护**

NSFOCUS NIPS 提供对应用层的防护功能，针对操作系统、应用软件以及数据库，提供深度的内容检测技术、过滤报文里的恶意流量和攻击行为，保护存在的漏洞，防止操作系统和应用程序损坏或宕机。

◆ **内容管理**

NSFOCUS NIPS 对企业内部网络资源提供内容管理，可以有效检测并阻断间谍软件，包括木马后门、恶意程序和广告软件等，并可以对即时通讯、P2P 下载、网络游戏、在线视频、网络流媒体等内容进行监控并阻断。

二. 基础知识

2.1 接口

接口是指网络物理硬件接口的逻辑对象，拥有配置网络地址并进行网络通讯的能力。

◆ **双工模式**

网络接口的工作模式，有 **auto**（自动匹配）、**full**（全双工）和 **half**（半双工）三个选项。

◆ **连接速率**

强制接口的协商速率，可选项包括 **10MB**、**100MB** 和 **1000MB**。请根据与 NSFOCUS NIPS 引擎连接的网络设备的特性，选择适当的协商速率（默认为**自动协商**），以保证网络通讯正常。

2.2 子接口

子接口与物理接口相似，即信息流进出安全区的开口。从逻辑上讲，可以将一个物理接口分为几个虚拟子接口。

子接口必须与它的父接口在同一个安全区（此安全区类型为 layer3），它们的 IP 地址不能在同一网段。

2.3 安全区

根据接口的工作方式，配置接口所属的安全区，在同一安全区内的接口之间存在通讯上的关联。以下几种情况不允许修改所属安全区：

- 非千兆 intel 网卡的接口不允许修改所属安全区。
- 接口存在路由策略时不允许修改所属安全区。
- 证书存在问题时不允许修改所属安全区，例如：未导入证书之前不允许修改任何接口的所属安全区。
- 工作口数量已经达到证书允许的数量时，不允许再把非工作口改为工作口。
- 接口上配有子接口或映射规则时不允许修改所属安全区。

安全区是指拥有相同工作类型的接口的集合，包括以下五种工作类型：

透明（layer2）——配置在同一种安全区的多个接口处于二层交换工作模式。

路由（layer3）——配置在同一种的多个安全区之内的接口处于三层交换工作模式。

监听（monitor）——配置为该安全区的接口处于 IDS 监听工作模式。

直通（direct）——同一个安全区之内的接口处于 IPS 的 inline 工作模式。

管理（mgt）——配置为该安全区的接口只能用于带外管理。

global 是系统缺省的全区域，包含所有的安全区。

2.4 对象

对象，即将一些分散的同类型事物组合在一起，并给该组定义一个别名，这个别名就是对象的名称。管理员可以定义系统中所有对象，包括网络对象、服务对象、事件对象、IM/P2P 对象和时间对象。

通过对象的引入，可以更加灵活的配置策略。

2.5 VLAN 与 VLAN 路由

VLAN 即虚拟局域网（Virtual Local Area Network），是一种通过将局域网内的设备逻辑的而不是物理的划分成的一个个网段，从而实现虚拟工作组的新兴技术。VLAN 是为解决以太网的广播问题和安全性而提出的，它在以太网帧的基础上插入了一个 VLAN 头，用 VLAN ID 把用户划分为更小的工作组，限制不同工作组间的用户二层互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态管理网络。

VLAN 技术允许网络管理者将一个物理的 LAN 逻辑地划分成不同的广播域（即 VLAN），每个 VLAN 都包含一组相同需求的计算机工作站，与物理上形成的 LAN 具有相同的属性。但是，由于它是逻辑地而不是物理地划分，所以同一个 VLAN 内的各个工作站无需放置在同一个物理空间里，即这些工作站不一定属于同一个物理 LAN 网段。一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，即使是两台计算机具有相同的网段，但是它们却没有相同的 VLAN 号，它们各自的广播流也不会相互转发，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

VLAN 路由的作用是实现不同 VLAN 之间的通讯。

2.6 证书系统

NSFOCUS NIPS 的证书分为以下两类，它们的区别是：

◆ 试用证书

试用证书过期后，将无法继续使用本系统。

◆ 销售证书

销售证书过期后，可以继续使用本系统，但无法进行系统升级。

在 NSFOCUS NIPS 证书信息的“加载模块”一栏中，可以查看已购买的功能模块：默认模块是**防火墙+流量管理+抗拒绝服务+入侵防护**，另外，NSFOCUS NIPS 证书还可以控制工作口的使用个数，如果控制的接口个数少于系统自身的接口个数，那么多余的接口只能作为“带外管理”接口使用，并且不能改变该接口的安全区。

三. 登录引擎 Web 管理界面

3.1 登录方法

下面介绍登录 NSFOCUS NIPS 的 Web 管理界面的操作方法：

（1）确认客户端主机可以和 NSFOCUS NIPS 正常通讯（如果通过防火墙，请将 443 端口打开）。

（2）打开浏览器（例如：IE），用 HTTPS 方式连接 NSFOCUS NIPS 的 IP 地址，例如 *https://192.168.1.1*。

（3）回车后出现安全警报框，如图 3.1 所示（IE6.0 及以下版本会出现安全警报框），单击【是】，接受 NSFOCUS NIPS 证书加密的通道。

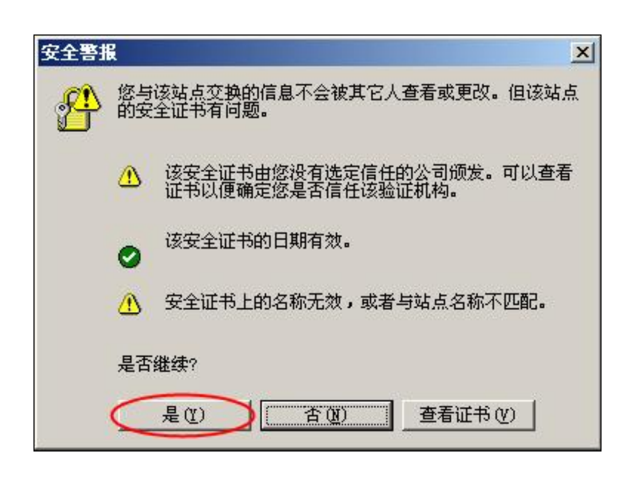


图 3.1 登录时的安全警报界面

（4）在如图 3.2 所示的 NSFOCUS NIPS 登录界面中，输入正确的用户名和密码，并单击【登录】。



图 3.2 NSFOCUS NIPS 的 Web 管理登录界面

（5）成功登录后，进入系统当前运行状态的界面，如图 3.3 所示。



图 3.3 NSFOCUS NIPS 当前的运行状态信息

 注意事项：

- 建议使用 IE6.0 或 Firefox2.0 以上版本的浏览器，屏幕分辨率最好设置为 1024×768 及以上。
- 初次使用本系统时可用默认用户登录，用户名和密码均是 weboper。建议首次登录后修改密码，具体操作方法请参见 9.4 帐号管理。
- 登录失败的原因有可能是：①用户名输入错误 ②密码输入错误 ③没区分大小写 ④帐户被禁用或删除。
- 登录本系统之前，请检查浏览器是否设置了禁止弹出窗口属性或者禁止 javascript，如果是，请撤销此设置。
- 用户登录后，如果不活动的时间超过 5 分钟，系统将超时并自动退回到登录页面，请重新登录继续使用。

3.2 导入证书

初次登录系统时，必须导入证书，否则无法使用本系统。

如图 3.4 所示，单击【浏览…】选取证书文件（*.lic），然后单击【导入证书】，系统会弹出证书信息确认对话框，如图 3.5 所示。如果确认证书状态正确，单击【确定】完成导入，否则单击【取消】返回，重新选择正确的证书。



图 3.4　导入引擎证书之前



图 3.5　导入引擎证书确认对话框

重启引擎后，NSFOCUS NIPS 的证书才能加载并生效。

3.3 系统状态确认

导入证书之后即可查看证书信息，或者进入菜单【系统】➔【证书管理】，确认系统状态，如图 3.6 所示。在证书状态中显示“正确”，表示证书已正确导入，系统状态正确，可以正常使用本系统；在证书状态中显示“错误”，表示证书有错误或未被正确导入，请联系绿盟科技的技术支持人员。

IPS ▸ 系统 ▸ 证书管理

证书管理

证书状态	正常
证书类型	试用证书
产品类型	ips
加载模块	入侵防护+防火墙+流量管理+IM/P2P
有效工作口数	不限
颁发给	007
颁发日期	2009-08-02
截止日期	2009-09-01

导入证书

图 3.6　正确导入引擎证书之后的证书信息

四. 部署方式

4.1 直通部署方式

4.1.1 单路部署

目前，很多企业从公司内网到外网有一条链路，通过单路部署 NSFOCUS NIPS 的方式，可以保护内网客户不受到来自 Internet 的攻击。

单路部署，即选择一对接口作为工作口为一路 Direct，任选一个接口为管理端口（也可以任选其中一个工作口作为管理端口），部署结构如图 4.1 所示。

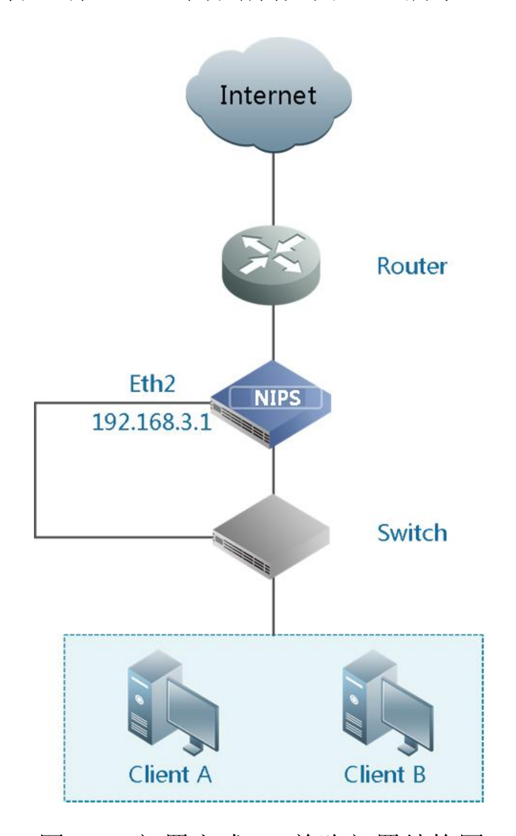


图 4.1 部署方式 – 单路部署结构图

假定内网网段地址是 192.168.3.0/24，管理口 IP 地址是 192.168.3.1，网关是 192.168.3.254，eth0 连接外网，eth1 连接内网，eth2 为管理端口。将 eth0 和 eth1 设置为一路 Direct-A 部署方式，Direct 接口 IP 在通讯中不起作用，但不能和管理口 IP 在同一网段，具体配置方法如下：

（1）选择菜单【网络】➔【接口】，进入接口列表的页面。

（2）配置 eth0 接口，如图 4.2 所示。



图 4.2 单路部署方式 – 配置 eth0 接口

（3）配置 eth1 接口，如图 4.3 所示。



图 4.3 单路部署方式 – 配置 eth1 接口

（4）配置 eth2 接口，如图 4.4 所示。

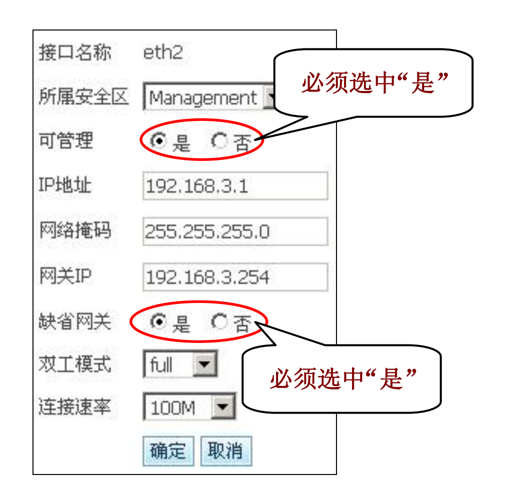


图 4.4 单路部署方式 – 配置 eth2 接口

（5）单路部署的接口配置完毕，返回接口列表，各项参数值如图 4.5 所示。

接口名称	是否可管理	接口IP	网络掩码	网关IP	双工模式	连接速率(Mb)	所属安全区	配置
eth0	否	192.168.10.186	255.255.255.0	192.168.10.254	Full	100Mb/s	Direct-A	
eth1	否	10.8.24.212	255.255.255.255	10.8.24.1	Full	100Mb/s	Direct-A	
eth2	是	192.168.3.1	255.255.255.0	192.168.3.254缺省	Full	100Mb/s	Management	

图 4.5 部署方式 – 单路部署的接口列表

4.1.2 多路部署

目前，很多企业为了保证网络带宽资源的充足和网络冗余，网络出口采用多链路连接方式，连接到两个或更多 ISP 服务商。针对这种连接方式，可以在网络出口处部署一台 NSFOCUS NIPS，采用多链路防护的部署方式。

多路部署，即选择两对接口配置为 Direct 接口，同时配置为管理接口 IP 地址，部署结构如图 4.6 所示。

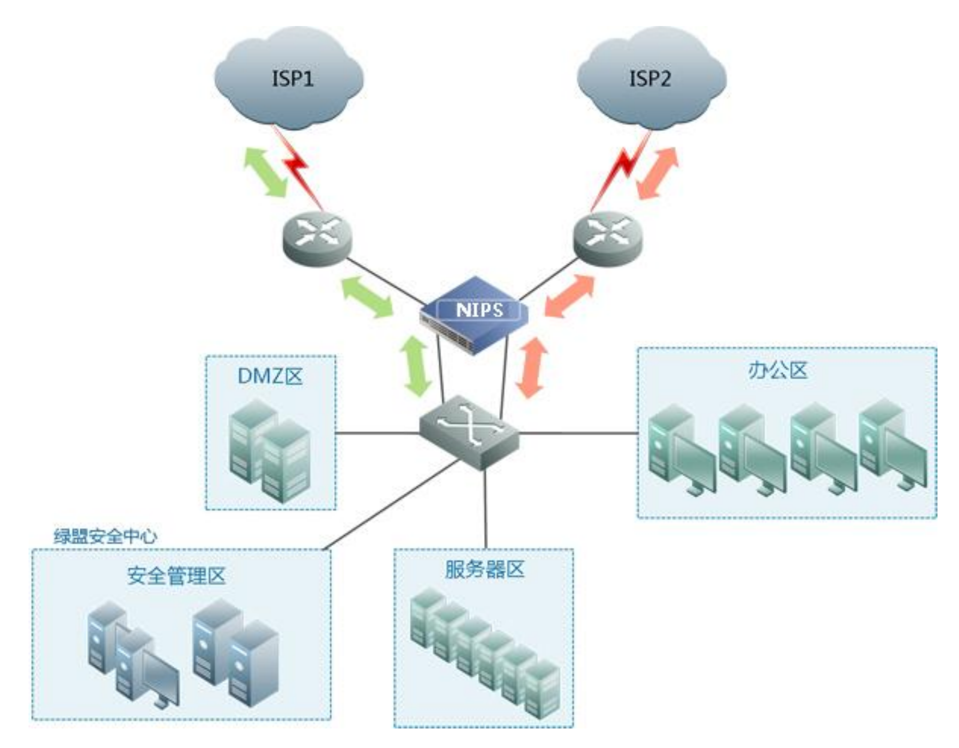


图 4.6 部署方式 – 多路部署结构图

假定内网网段地址是 192.168.3.0/24，管理口 IP 地址是 192.168.3.1，网关是 192.168.3.254，eth0 和 eth2 连接外网，eth1 和 eth3 连接内网，eth3 同时作为管理端口，具体配置方法如下：

（1）依次配置 eth0~eth3，以 eth3 为例，它的配置页面如图 4.7 所示。

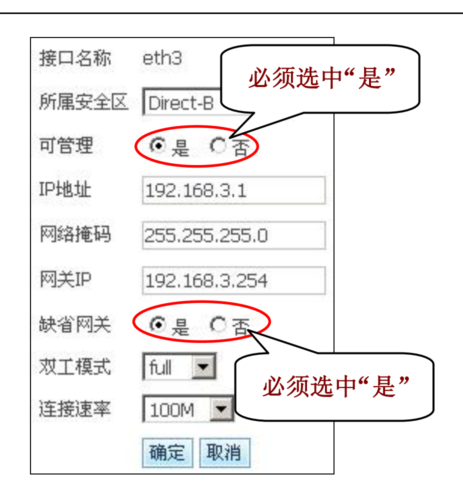


图 4.7 多路部署方式 – 配置 eth3 接口

（2）多路部署的接口配置完毕，返回接口列表，各项参数值如图 4.8 所示。

接口名称	是否可管理	接口IP	网络掩码	网关IP	双工模式	连接速率(Mb)	所属安全区	配置
eth0	否	192.168.10.186	255.255.255.0	192.168.10.254	Full	100Mb/s	Direct-A	
eth1	否	200.200.200.0	255.255.255.255	200.200.200.254	Full	100Mb/s	Direct-A	
eth2	否	192.168.2.1	255.255.255.0	192.168.2.254	Full	100Mb/s	Direct-B	
eth3	是	192.168.3.1	255.255.255.0	192.168.3.254缺省	Full	100Mb/s	Direct-B	

图 4.8 部署方式 – 多路部署的接口列表

4.2 三层部署方式

目前，很多企业网络连接到互联网的方式是在网络边界部署路由器、防火墙以及入侵防护系统，串联的设备比较多，造成网络边界单点故障率日益增多，影响整个网络的稳定性。

针对这种连接方式，可以使用三层部署方式，将 NSFOCUS NIPS 部署在网络边界。它类似于一个路由器，同时提供静态路由、动态路由和策略路由；同时，它又是一台防火墙，实现 NAT 地址转换和流量管理，提供网络层安全防护；另外，它还是一台入侵防护系统，实现应用层和内容层的安全防御。也就是配置内网、外网和 DMZ 区域的三个接口，实现 NAT 和一一映射。

4.2.1 静态路由部署

目前，很多企业从公司内网到外网有一条链路，通过单路部署 NSFOCUS NIPS 的方式，可以保护内网客户不受到来自 Internet 的攻击。

静态路由部署，即配置内网、外网和 DMZ 三个区域，部署结构如图 4.9 所示。

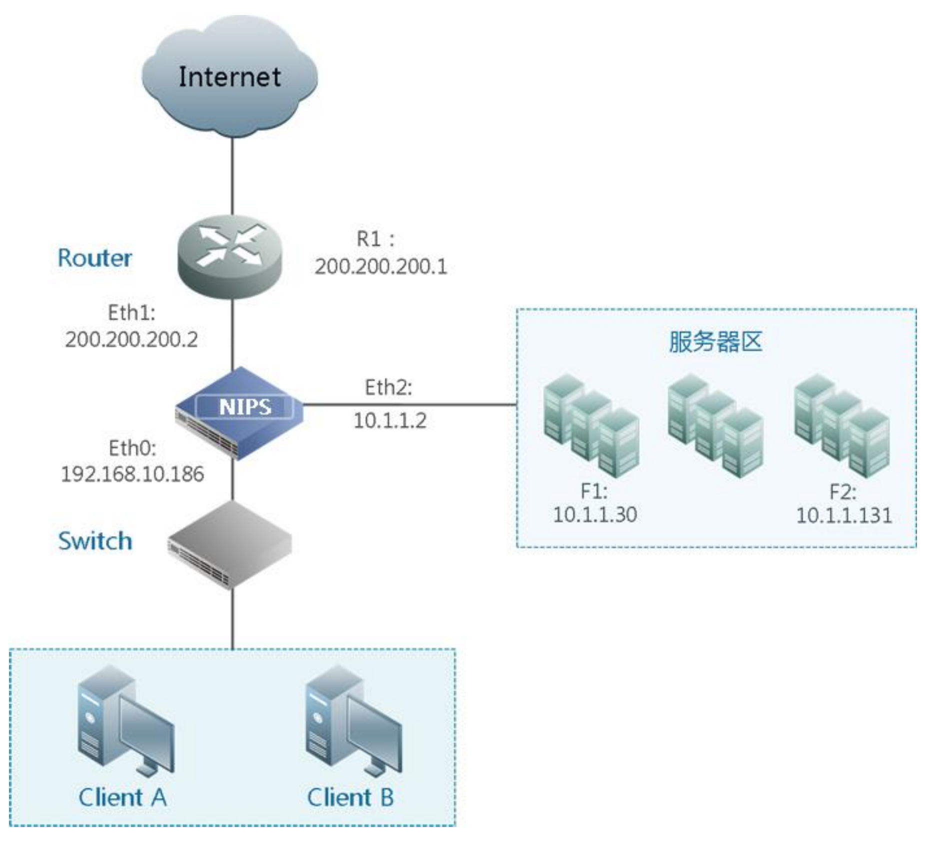


图 4.9 部署方式 – 静态部署结构图

假定 eth0 连接内网，eth1 连接外网，eth2 连接 DMZ 区域，它们的具体参数配置如下：

- eth0 连接内网的 IP 地址是 192.168.10.186/24，该内网网段还包括 192.168.1.0/24 和 192.168.2.0/24 两个网段，内网接口网关是 192.168.10.254；
- eth1 连接外网的 IP 地址是 200.200.200.2/255.255.255.248，外网路由设备 R1 的 IP 地址是 200.200.200.1；
- eth2 连接 DMZ 区域的 IP 地址是 10.1.1.2，DMZ 区域内的两台服务器需要开放从外网访问的权限，其中 F1（10.1.1.30）对外开放所有端口，F2（10.1.1.131）只对外开放 80 端口；
- 200.200.200.3-6 作为剩余获取的公网 IP 地址。

1. 配置安全区

选择菜单【网络】➔【安全区】，进入安全区列表的页面，依次配置以下内容：

（1）配置 DMZ 安全区，如图 4.10 所示。



图 4.10　静态路由部署方式 – 配置 DMZ 安全区

（2）配置内网安全区，如图 4.11 所示。



图 4.11　静态路由部署方式 – 配置内网安全区

（3）配置外网安全区，如图 4.12 所示。



图 4.12　静态路由部署方式 – 配置外网安全区

2.　配置接口

选择菜单【网络】➔【接口】，进入网络接口的页面，依次配置以下内容：

（1）配置内网接口 eth0，如图 4.13 所示。



图 4.13　静态路由部署方式 – 配置内网接口

（2）配置外网接口 eth1，如图 4.14 所示。

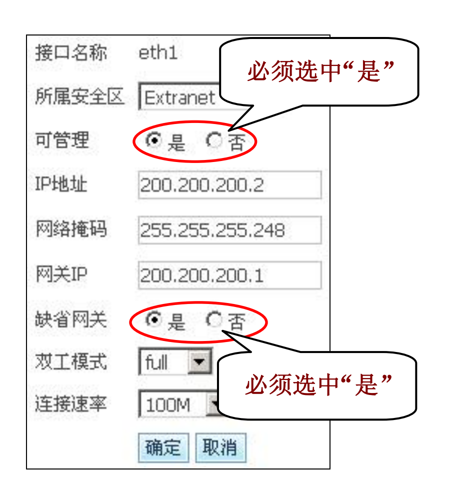


图 4.14 静态路由部署方式 – 配置外网接口

（3）配置 DMZ 安全区接口 eth2，如图 4.15 所示。



图 4.15 静态路由部署方式 – 配置 DMZ 安全区接口

（4）接口配置完毕，返回接口列表，如图 4.16 所示。

接口名称	是否可管理	接口IP	网络掩码	网关IP	双工模式	连接速率(Mb)	所属安全区	配置
eth0	否	192.168.10.186	255.255.255.0	192.168.10.254	Full	100Mb/s	Intranet	
eth1	是	200.200.200.2	255.255.255.248	200.200.200.1缺省	Full	100Mb/s	Extranet	
eth2	否	10.1.1.2	255.255.255.0	10.1.1.254	Full	100Mb/s	DMZ	

图 4.16 静态路由部署方式 – 配置完成后的接口列表

3. 配置对象

在配置 NAT、端口映射和一一映射之前，必须先创建对象，包括 NAT 使用的 IP 地址或 IP 地址池、内部服务器的 IP 地址、映射后使用的公网 IP 地址等。

选择菜单【对象】➔【网络】，进入配置网络对象的页面，依次配置以下内容：

（1）创建节点对象（DMZ 服务器），作为一一映射的服务器，如图 4.17 所示。



图 4.17 静态路由部署方式 – 创建节点对象（DMZ 服务器）

（2）创建节点对象（一一映射公网的 IP 地址），如图 4.18 所示。



图 4.18 静态路由部署方式 – 创建节点对象（一一映射公网的 IP 地址）

（3）创建节点对象（DMZ 区域的 Web 服务器内部 IP 地址），如图 4.19 所示。



图 4.19 静态路由部署方式 – 创建节点对象（DMZ 区域的 Web 服务器内部 IP 地址）

（4）创建节点对象（外网接口 IP 地址），作为端口映射的公网 IP 地址，如图 4.20 所示。



图 4.20 静态路由部署方式 – 创建节点对象（外网接口 IP 地址）

（5）节点对象配置完毕，返回节点对象列表，如图 4.21 所示。

网络 节点 IP池 组

每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	网络	备注	取反	配置
1501	DMZ服务器	10.1.1.30		否	
1502	一一映射公网的IP地址	200.200.200.3		否	
1503	DMZ区域的Web服务器内部IP地址	10.1.1.131		否	
1504	外网接口IP地址	200.200.200.2		否	

图 4.21 静态路由部署方式 – 配置完成后的节点对象列表

（6）配置 NAT 使用的外网 IP 地址池（也可以使用外网接口 IP 地址），如图 4.22 所示。



图 4.22 静态路由部署方式 – 创建 IP 池对象（NAT 使用地址）

（7）NAT 使用地址对象配置完毕，返回 IP 池对象列表，如图 4.23 所示。



网络 节点 IP池 组

每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	网络	备注	取反	配置
1	NAT使用地址	200.200.200.4 - 200.200.200.5		否	

图 4.23 静态路由部署方式 – 配置完成后的 IP 池对象列表

4.　NAT 配置

选择菜单【策略】➔【防火墙】➔【防火墙策略】，进入防火墙规则列表的页面，依次配置以下内容：

（1）创建一条防火墙规则，如图 4.24 所示。



图 4.24　静态路由部署方式 – 配置防火墙规则的 NAT

（2）创建完毕，返回防火墙规则列表，如图 4.25 所示。在“选项”一栏下出现图标表示该条防火墙规则中使用 NAT 转换地址对象。



编号	源对象	目的对象	服务	动作	选项	使用	配置
1	any	any	any				

图 4.25　静态路由部署方式 – 配置完成后的防火墙规则列表

5.　一一映射配置

选择菜单【网络】➔【接口】，进入外网接口 eth1 的编辑页面，依次配置以下内容：

（1）创建 eth1 的一一映射规则，如图 4.26 所示。



图 4.26 静态路由部署方式 – 配置外网接口的一一映射规则

（2）配置完毕，返回 eth1 的一一映射规则列表，如图 4.27 所示。

接口信息 | 一一映射 | 端口映射 | 子接口配置

每页显示 20 | 前一页 | 1/1 | 后一页 | 刷新 | 新建

是否使用	编号	内部对象	外部对象	选项	备注	配置
☑	1	DMZ服务器	一一映射公网的IP地址			

图 4.27 静态路由部署方式 – 配置完毕的外网接口一一映射规则列表

（3）创建一条“外网→外网”的防火墙规则，如图 4.28 所示。



图 4.28 静态路由部署方式 – 创建“外网→外网”的防火墙规则

6. 端口映射配置

选择菜单【网络】→【接口】，进入外网接口 eth1 的编辑页面，依次配置以下内容：

（1）创建 eth1 的端口映射规则，如图 4.29 所示。



图 4.29 静态路由部署方式 – 配置外网接口的端口映射规则

（2）配置完毕，返回 eth1 的端口映射规则列表，如图 4.30 所示。



是否使用	编号	内部对象	内部端口	外部对象	外部端口	协议	选项	备注	配置
☑	1	DMZ区域的Web服务器内部IP地址	80	外网接口IP地址	80	tcp			

图 4.30 静态路由部署方式 – 配置完毕的外网接口端口映射规则列表

（3）创建一条“外网→外网”的防火墙规则，如图 4.28 所示。

7. 静态路由配置

若要访问内网 192.168.1.0/24 和 192.168.2.0/24 的两个网段，必须添加静态路由信息，由于该网段不在接口路由中，所以需要手工添加，依次配置以下内容：

（1）选择菜单【网络】→【路由】→【静态路由】，创建内网接口的静态路由，如图 4.31 和图 4.32 所示。



图 4.31 静态路由部署方式 – 创建静态路由 1



图 4.32 静态路由部署方式 – 创建静态路由 2

（2）内网接口的静态路由创建完毕，返回静态路由列表，如图 4.33 所示。



静态路由 策略路由 OSPF

每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	目标IP	目标掩码	网关	接口	优先级	配置
1	1	192.168.1.10	255.255.255.0	192.168.10.254	eth0	2	
2	2	192.168.2.10	255.255.255.0	192.168.10.254	eth0	2	

图 4.33 静态路由部署方式 – 配置完毕的静态路由列表

（3）静态路由配置完毕，192.168.1.0 和 192.168.2.0 这两个网段的内网地址即可正常访问外网和 DMZ 区域。

4.2.2 OSPF 动态路由部署

动态路由部署结构与静态路由的部署相似，不同之处是部署在 OSPF 的动态网络路由中。

与 CISCO IOS 管理界面类似，通过串口或者 SSH 方式连接 NSFOCUS NIPS 的 50022 端口并登录（初始用户名和密码均是 shell，通过 SSH 方式需要打开远程协助）。

4.2.2.1 动态路由部署方式一

如图 4.34 所示，NSFOCUS NIPS 既作为 NAT 设备使内网用户可以连接外网网络，同时也通过 OSPF 为两个网络提供路由。

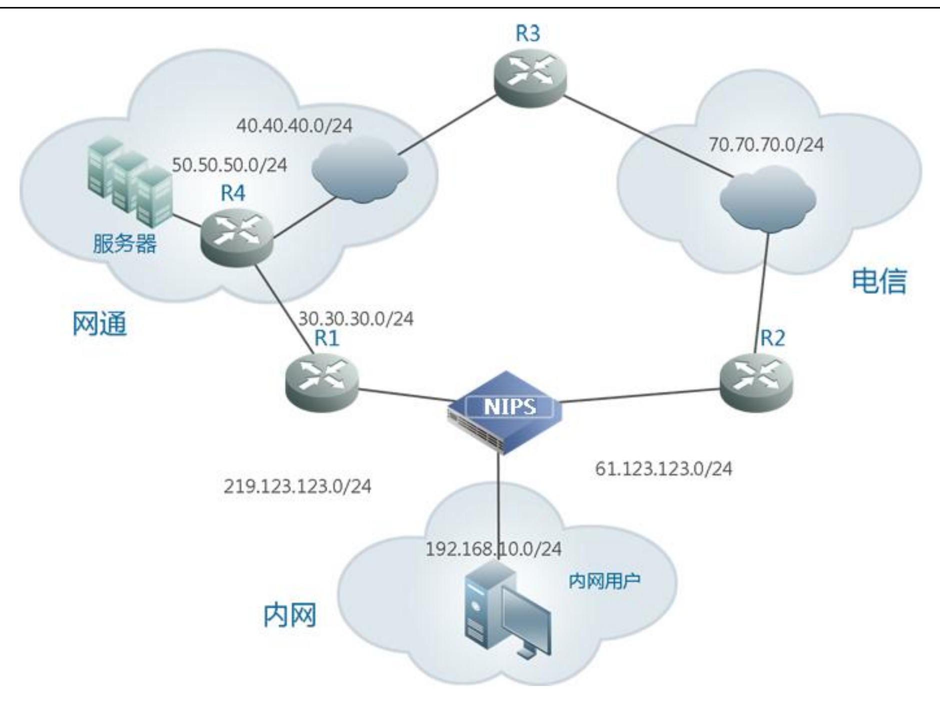


图 4.34 部署方式 – 动态路由部署结构图（方式一）

这种动态路由部署方式需要配置以下信息：

（1）登录 NSFOCUS NIPS 的 Web 管理界面，分别配置连接 R1、R2 路由器和内网接口的 IP 地址，内网接口的安全区类型设置为 layer3。注意：这些接口必须设为可管理。

（2）选择菜单【策略】➔【防火墙】，配置两条防火墙规则，规则中使用内网地址的 NAT 转换地址。

（3）通过 SSH 方式连接 NSFOCUS NIPS，登录 CLI 管理界面，配置 OSPF 路由（配置方法与 CISCO 路由器的相同），如下所示。

```
Hello, this is Shell.
localhost>enable
localhost# configure terminal
localhost (config)# router ospf
localhost (config-router)# network 219.123.123.0/24 area 0
localhost (config-router)# network 61.123.123.0/24 area 0
```

4.2.2.2 动态路由部署方式二

如图 4.35 所示，NSFOCUS NIPS 充当连接多个 OSPF 区域的 ABR（区域边界路由器），另外在区域 1 还存在末梢区域。

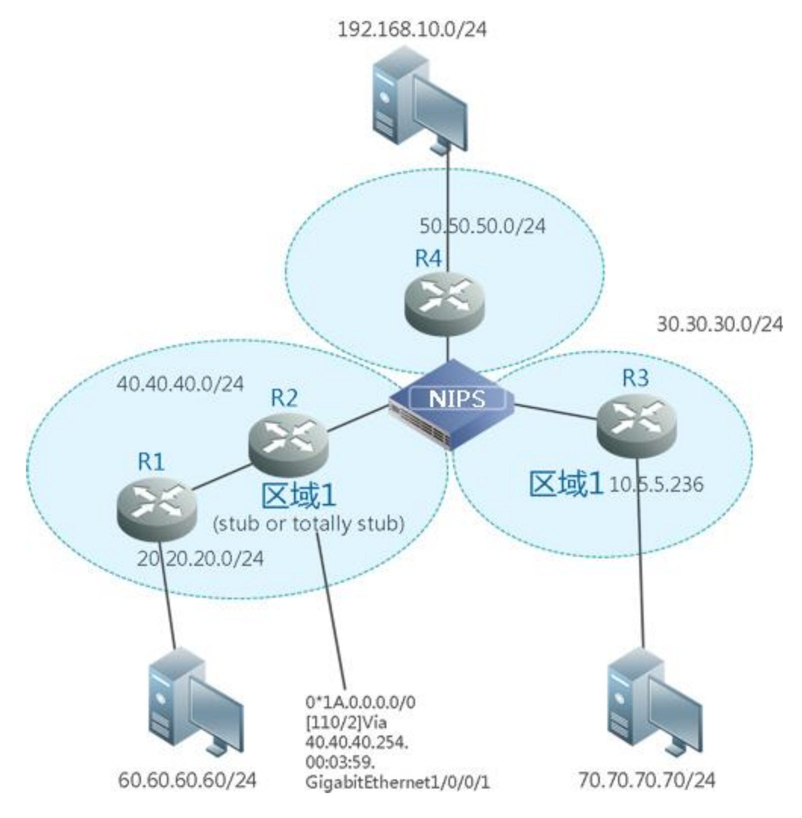


图 4.35 部署方式 – 动态路由部署结构图（方式二）

这种动态路由部署方式需要配置以下信息：

（1）登录 NSFOCUS NIPS 的 Web 管理界面，分别配置连接 R2、R3 和 R4 路由器的 IP 地址，接口的安全区类型设置为 layer3（为了应用策略方便，最好不要将三个接口配置为同一安全区）。

（2）通过 SSH 方式连接 NSFOCUS NIPS，登录 CLI 管理界面，配置 OSPF 路由（配置方法与 CISCO 路由器的相同），如下所示。

```
Hello, this is Shell .
localhost>enable
localhost# configure terminal
localhost (config)# router ospf
localhost (config-router)# network 30.30.30.0/24 area 10.5.5.236
localhost (config-router)# network 40.40.40.0/24 area 1
localhost(config-router)# network 50.50.50.0/24 area 0
localhost(config-router)# area 1 stub no-summary -- 完全末梢区域
```

NSFOCUS NIPS 的 CLI 界面与 CISCO IOS 的基本相同，只是部分功能有所简化。使用命令时可以直接加“?”来获取帮助信息。有关接口和安全区的配置方法，请参见 4.2.1 静态路由部署。

以上两个动态路由部署方式均为最简单的配置，具体情况需根据客户使用 OSPF 的方式来设置其他参数，生成的 OSPF 路由信息可以登录 Web 管理界面，选择菜单【网络】➔【路由】➔【OSPF】进行查看，如图 4.36 所示。

编号	目标IP	目标网络掩码	网关IP	优先级	接口
0	60.60.60.0	255.255.255.0	40.40.40.254	10	eth0
1	20.20.20.0	255.255.255.0	40.40.40.254	20	eth0
2	192.168.10.0	255.255.255.0	50.50.50.254	10	eth1
3	70.70.70.0	255.255.255.0	30.30.30.254	10	eth2

图 4.36 部署方式 – 查看 OSPF 路由信息

4.2.3 RIP 动态路由部署

RIP 的部署和 OSPF 的部署方法基本相同，具体拓扑部署请参见 4.2.2.1 动态路由部署方式一。

登录 CLI 管理界面后，配置 RIP 的命令如下所示：

```
Hello, this is Shell .
localhost>enable
localhost# configure terminal
localhost (config)# router rip
localhost (config-router)# network 219.123.123.0/24
localhost (config-router)# network 61.123.123.0/24
```

4.3 BGP 部署

BGP(Border GatewayProtocol)是边界网关路由选择协议，它可以实现两个自治域系统之间的路由选择。

BGP 的典型部署结构如图 4.37 所示。两个自治域不同的网络使用了不同的 IGP 路由协议。As 100 自治域内部使用 RIP 协议，而 As 200 自治域内部使用 OSPF 协议，两个自治域

网络通过 BGP 路由协议交换相互自治域内的 IGP 路由信息。

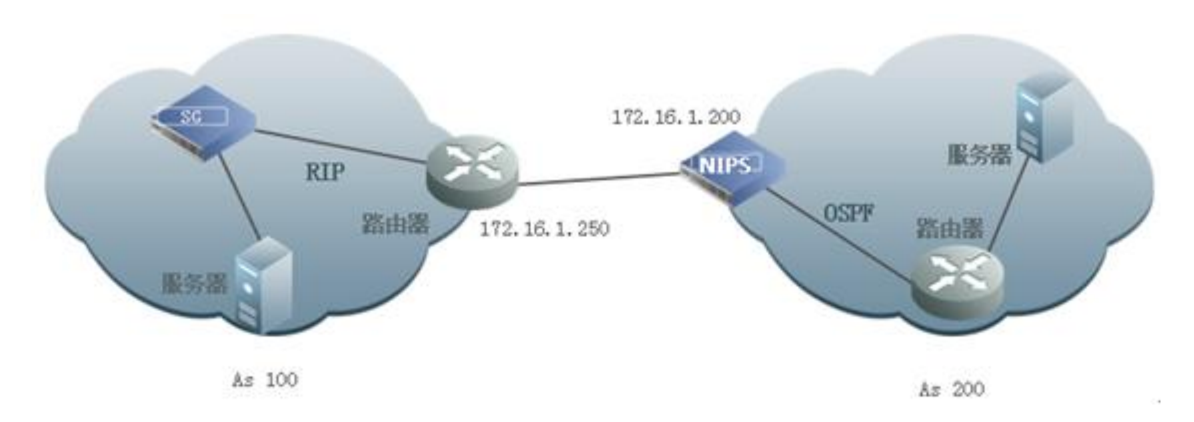


图 4.37 部署方式 – BGP 部署结构图

在 As 200 自治域中的 NIPS 设备上，BGP 部署的配置信息如下：

（1）登录 NSFOCUS NIPS 的 Web 管理界面，分别配置 NIPS 设备和路由器的 IP 地址。

（2）通过 SSH 方式连接 NSFOCUS NIPS，登录 CLI 管理界面，配置 BGP 路由（配置方法与 CISCO 路由器的相同），如下所示。

```
Hello, this is Shell .
localhost>enable
localhost# configure terminal
localhost (config)# router ospf
localhost (config-router)# network 61.123.123.0/24 area 0.0.0.0
localhost (config-router)# exit
localhost (config-router)# router bgp 200
localhost (config-router)# bgp router-id 10.14.20.200
localhost (config-router)# redistribute ospf
localhost (config-router)# neighbor 172.16.1.250 remote-as 100
```

4.4 VLAN 部署

在 VLAN 网络中的部署方式是将 NSFOCUS NIPS 架设在 VLAN 之间，通过安全策略检查之后才允许不同 VLAN 之间的数据传输。

4.4.1 VLAN 部署方式一：隔离广播域

这种 VLAN 部署的结构如图 4.38 所示。

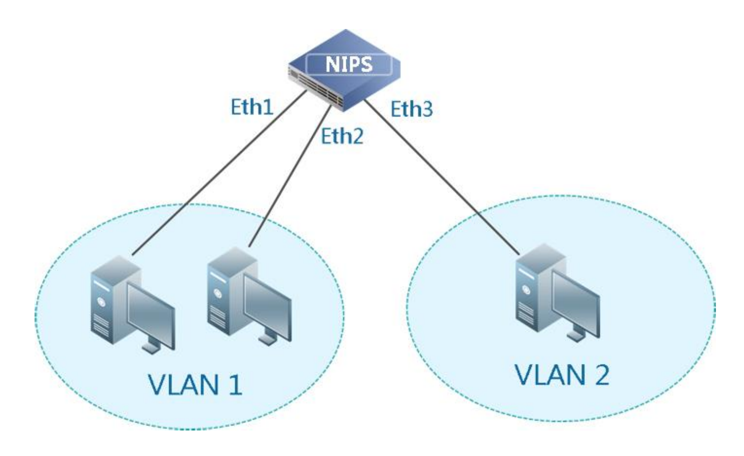


图 4.38 部署方式 – VLAN 部署结构图（隔离广播域）

配置以下信息：

（1）选择菜单【网络】➔【安全区】，创建两个 Access 模式的 layer2 安全区 VLAN_A 和 VLAN_B，它们的 VLAN ID 分别设为 1 和 2，安全区的路由设置为否，如图 4.39 和图 4.40 所示。

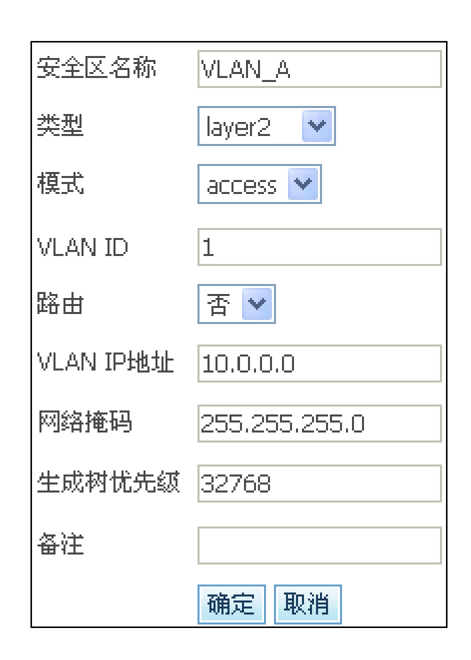


图 4.39 VLAN 部署 – 创建 Access 模式的安全区 VLAN_A

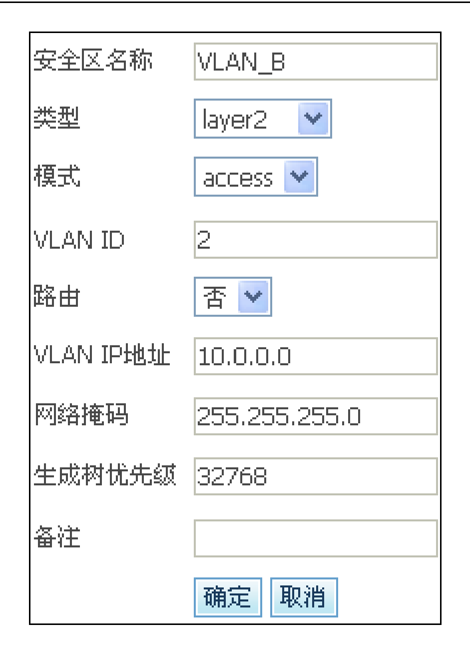


图 4.40 VLAN 部署 – 创建 Access 模式的安全区 VLAN_B

（2）将 VLAN_A 分配给接口 eth1 和 eth2，将 VLAN_B 分配给接口 eth3，如图 4.41 所示。

接口名称	是否可管理	接口IP	网络掩码	网关IP	双工模式	连接速率(Mb)	所属安全区	配置
eth0	是	192.168.10.186	255.255.255.0	192.168.10.254	full	100	Management	
eth1	否	200.200.200.2	255.255.255.248	200.200.200.1 缺省	full	100	VLAN_A	
eth2	否	10.1.1.2	255.255.255.0	10.1.1.254	full	100	VLAN_A	
eth3	否	192.168.11.22	255.255.255.0	192.168.11.101	full	100	VLAN_B	

图 4.41 VLAN 部署 – 隔离广播域的接口列表

（3）eth1 和 eth3 连接的设备之间无法通讯，eth1 和 eth2 连接的设备之间可以相互通讯，即产生隔离广播域的作用。

4.4.2 VLAN 部署方式二：Trunk

这种 VLAN 部署的结构如图 4.42 所示。

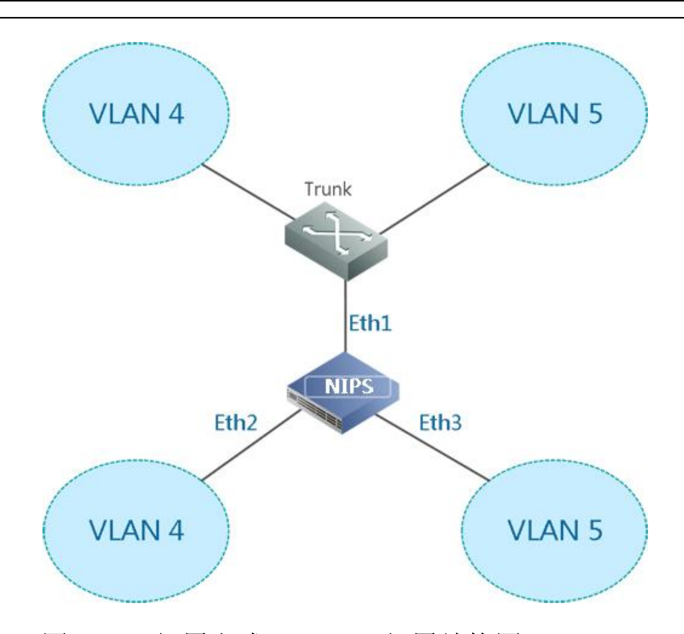


图 4.42 部署方式 – VLAN 部署结构图（Trunk）

配置以下信息：

（1）选择菜单【网络】➔【安全区】，创建一个 Trunk 模式的 layer2 安全区 VLAN_C，默认的 VLAN ID 是 4，支持的 VLAN 是 4-5，如图 4.43 所示。



图 4.43 VLAN 部署 – 创建 Trunk 模式的安全区 VLAN_C

（2）操作方法同上，创建两个 Access 模式的 layer2 安全区 VLAN_D 和 VLAN_E，分别划分给 VLAN 4 和 VLAN 5，安全区的路由设置为否。

（3）将 VLAN_C 分配给接口 eth1，将 VLAN_D 分配给接口 eth2，将 VLAN_E 分配给 eth3。

（4）在交换机和 NSFOCUS NIPS 两侧的同一 VLAN 的设备之间可以相互通讯。

4.4.3 VLAN 部署方式三：Trunk 穿越

这种 VLAN 部署的结构如图 4.44 所示，将两个工作口配置为 Direct 部署方式即可。

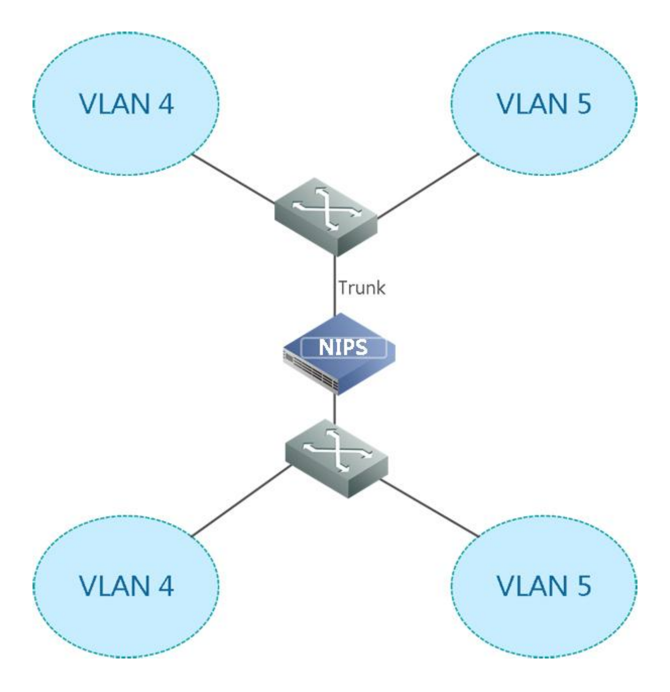


图 4.44 部署方式 – VLAN 部署结构图（Trunk 穿越）

4.4.4 VLAN 部署方式四：混合部署

这种 VLAN 部署的结构如图 4.45 所示。

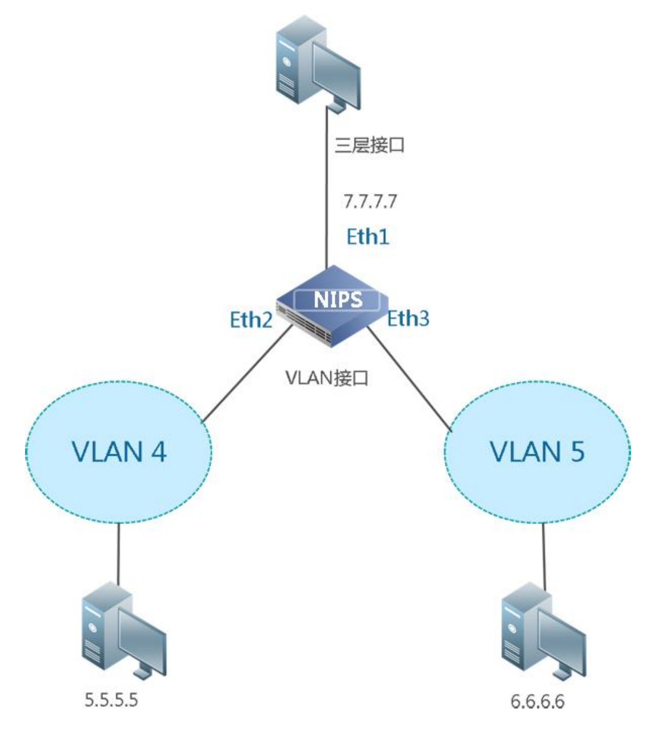


图 4.45 部署方式 – VLAN 部署结构图（混合部署）

配置以下信息：

（1）选择菜单【网络】➔【安全区】，创建一个三层模式的安全区 VLAN_F，如图 4.46 所示。



图 4.46 VLAN 部署 – 创建三层模式的安全区 VLAN_F

（2）操作方法同上，创建两个 Access 模式的 layer2 安全区 VLAN_G 和 VLAN_H，它们的 VLAN ID 分别设为 4 和 5，安全区的路由设置为**是**，VLAN_G 的配置页面如图 4.47 所示。



图 4.47 VLAN 部署 – 创建 Access 模式的安全区 VLAN_G

（3）将安全区 VLAN_F 分配给接口 eth1 并连接网段 7.7.7.0/24，将安全区 VLAN_G 分配给接口 eth2，将安全区 VLAN_H 分配给 eth3。

（4）选择菜单【策略】➔【防火墙】➔【防火墙策略】，配置两条防火墙规则，分别是安全区 VLAN_G 到安全区 VLAN_F 以及安全区 VLAN_H 到安全区 VLAN_F，规则中使用内网地址的 NAT 转换地址。

4.5 单臂路由部署方式

单臂路由部署方式的结构如图 4.48 所示。

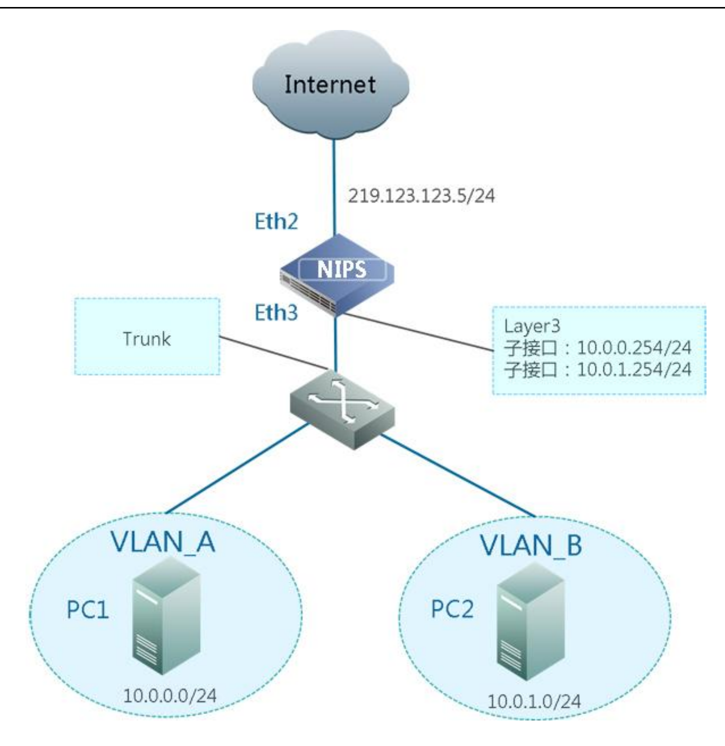


图 4.48 部署方式 – 单臂路由部署结构图

选择菜单【网络】➔【接口】，将 NSFOCUS NIPS 的接口 eth3 设置为三层安全区，并为其创建两个子接口，它们的 VLAN ID 分别设为 1 和 2，配置完毕的子接口列表如图 4.49 所示。

接口信息 一一映射 端口映射 子接口配置

每页显示 20 前一页 1/1 后一页 刷新 新建

IP地址	网络掩码	VLAN ID	配置
10.0.0.254	255.255.255.0	1	
10.0.1.254	255.255.255.0	2	

图 4.49 单臂路由部署方式 – 子接口列表

由于接口为三层接口，两个 VLAN 之间的路由会由 NSFOCUS NIPS 自动生成，实现 VLAN 1 和 VLAN 2 之间的正常通讯。

4.6 负载均衡部署方式

为了提高服务器的整体处理能力，并提高其可靠性、可用性和可维护性，从而达到加快服务器的响应速度，提高用户体验度的目的，可以采用负载均衡的部署方式。

假定某企业有三台 WEB 服务器同时提供 WEB 服务，网络部署方式的结构如图 4.50 所示。企业内网的地址为保留地址 10.10.10.2/24-10.10.10.50/24，企业的对外服务器的内部地址为 192.168.10.101-192.168.10.103，防火墙的内端口地址为 10.10.10.1，防火墙外网地址为 202.100.100.3。NIPS 设备接口连接方式如下：eth2 连接外网，eth1 连接内网，eth3 连接服务器 DMZ 区。

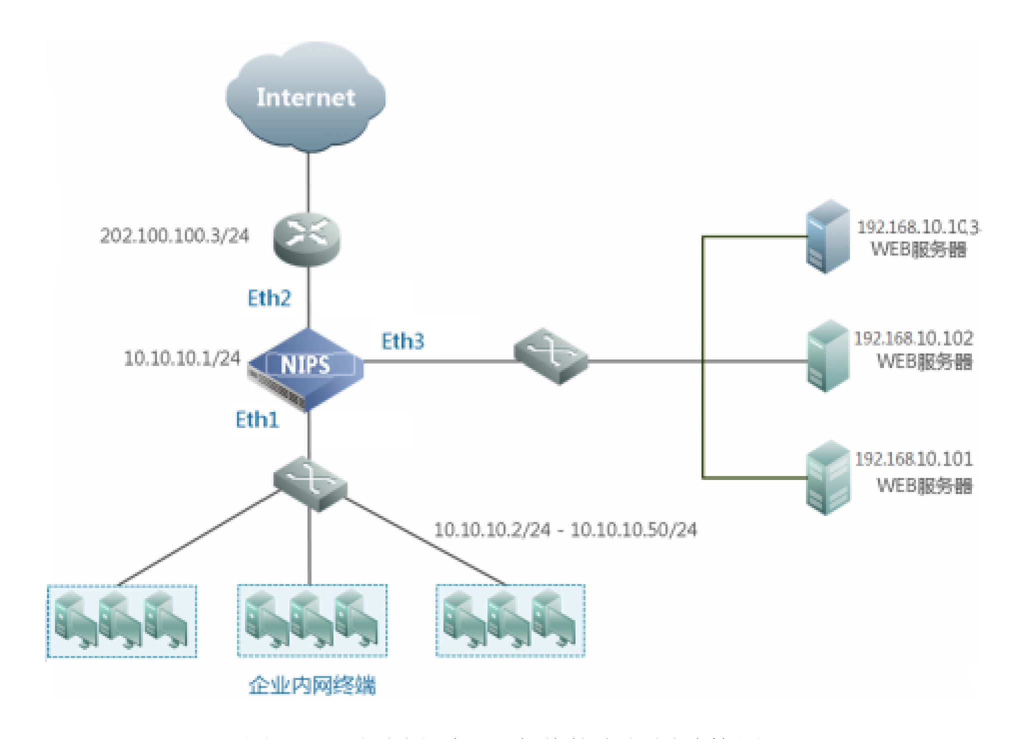


图 4.50 部署方式 – 负载均衡部署结构图

为使这三台服务器能对外提供 WEB 服务并分担负载，可以采用端口映射配置负载均衡的方式来实现。

具体配置方法如下：

步骤 1：新建一个 IP 池对象，开始地址为 192.168.10.101，结束地址为 192.168.10.103，配置方法请参见 5.1.1.4 IP 池对象。

步骤 2：添加内部地址映射到的公网地址对象。新建一个节点对象，IP 地址为 202.100.100.2，配置方法请参见 5.1.1.2 节点对象。

步骤 3：选择菜单【网络】➔【接口】➔【端口映射】，配置 eth2 接口，选择负载均衡的方式，具体配置方法请参见 5.3.4.2 端口映射。

⚠负载均衡的方式有两种：随机和轮询。选择随机方式，表示不同服务器之间响应外网的方式是随机的；选择轮询方式，表示不同服务器之间以一定的次序轮流响应外网的访问。

4.7 高可用性设置

4.7.1 高可用性 HA 设置

◆ **HA 简介**

高可用性 HA（High Availability），是指通过尽量缩短因日常维护操作（计划）和突发的系统崩溃（非计划）所导致的停机时间，以提高系统和应用的可用性。HA 系统是目前企业防止核心计算机系统因故障停机的最有效手段。

设备的 HA 采用主从/主主工作方式，可以实现如下功能：

- 链路状态的监测。
- 配置策略的同步。
- Session 的同步。

◆ **HA 配置**

选择菜单【网络】➔【高可用性设置】，即可进行高可用性设置即 HA 机制（双机热备）的配置，如图 4.51 所示。



图 4.51 网络 – 高可用性设置

其中各项参数含义如下：

启动 HA/停止 HA——NSFOCUS NIPS 支持 HA 机制，即需要两台 NSFOCUS NIPS 设备来实现双机热备功能。请选择是否启用该机制。只有 HA 没有启动的时候才能对 HA 机制的各项参数进行设置。

本机系统状态——显示当前 NSFOCUS NIPS 的系统状态。

对端系统状态——显示对端 NSFOCUS NIPS 的系统状态。

工作模式——本机启用 HA 机制后所处的地位，是**主机**还是**从机**（备份机），以及工作模式是**主动-主动**还是**主动-被动**。

心跳接口——本机连接对端 NSFOCUS NIPS 的接口。

对端 IP 地址——对端 NSFOCUS NIPS 心跳接口的 IP 地址。

心跳时间间隔——发送信号到对端 NSFOCUS NIPS 接口的时间间隔（推荐值：1000 毫秒）。

失去心跳次数——当对端 NSFOCUS NIPS 接口的信号丢失次数超过设定值时，认为连接断开。

会话同步——选择是否将当前 NSFOCUS NIPS 的会话信息与对端 NSFOCUS NIPS 进行同步。

防火墙策略同步——选择是否将当前 NSFOCUS NIPS 的防火墙策略与对端 NSFOCUS NIPS 的同步。

入侵防护策略同步——选择是否将当前 NSFOCUS NIPS 的入侵防护策略与对端 NSFOCUS NIPS 的同步。

对象配置同步——选择是否将当前 NSFOCUS NIPS 的对象配置信息与对端 NSFOCUS NIPS 的同步。

设置完毕，单击【启动 HA】会弹出重启引擎的确认信息。只有在启用了 HA 之后，单击【同步对端配置】，才能将对端 NSFOCUS NIPS 的配置信息与当前 NSFOCUS NIPS 的配置信息强制同步。

4.7.2 生成树配置

◆ 生成树协议简介

生成树协议 STP(Spanning Treep Protocol)是一种链路管理协议。它为网络提供路径冗余，使两个终端之间只有一条有效路径，有效防止网络产生环路。

◆ 生成树配置

具体配置步骤如下：

步骤 1：选择菜单【网络】➔【接口】，配置两个 layer2 型的接口。

步骤 2：选择菜单【网络】➔【生成树配置】，即可进行生成树参数的配置，如图 4.52 所示。

各项参数的含义如下：

心跳时间——发送交换桥协议数据单元 BPDU（Bridge Protocol Data Unit）的时间间隔，缺省值为 2s。

最大时间——收到报文的最长时间间隔。超过这个时间的报文，系统将直接丢弃，缺省值为 20s。

转发延迟——系统从学习状态转换到转发状态花费的时间，缺省值为 15s。

. **步骤 3**：设置完毕，单击【提交】，提交生成树配置的参数。

步骤 4：单击生成树配置界面上方的按钮【启动生成树】，弹出重启引擎的确认信息。单击【确认】，启动生成树的配置。

高可用性设置 | 生成树配置

生成树控制
启动生成树
停止生成树

生成树状态

生成树配置
心跳时间(hello time) 2
最大时间(max age) 20
转发延迟(forward delay) 15
提交

最大时间必须小于2*(转发延迟-1)
最大时间必须大于或等于2*(心跳时间+1)

图 4.52　网络－生成树配置

五. 策略配置

NSFOCUS NIPS 的策略配置包括防火墙策略、流量管理策略、入侵防护策略、IM/P2P 策略、内容安全策略、WEB 安全策略和防病毒策略的配置。添加策略之前，需要先配置对象的内容。

5.1 对象

对象，即将一些分散的同类型事物组合在一起，并给该组定义一个别名，这个别名就是对象的名称。管理员在此可以定义系统中所有对象，包括网络对象、服务对象、事件对象、IM/P2P 对象和时间对象。

5.1.1 网络对象

在设置所有策略及一一映射规则或端口映射规则时，需要引用网络对象来定义规则，共分为以下五类网络对象：网络、节点、MAC 地址、IP 池和网络组。

选择菜单【对象】➔【网络】，进入网络对象的设置页面。通过单击页面首部的标签，可以切换到相应的网络对象列表。

5.1.1.1 网络对象

这里的网络是指一个网段，即根据 IP 和网络掩码来指定的 IP 子网对象。

如图 5.1 所示，列出当前所有 IP 子网对象，其中 any 是系统缺省的网络对象，不能编辑或删除。对于无法删除的网络对象，表示已包含在网络组对象中或者正被某些规则使用，无论规则是否启用。


每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	网络	备注	取反	配置
301	any	0.0.0.0/0.0.0.0	Default	否	
302	TAP	172.168.0.0/255.255.0.0		否	
303	192.168.255.0	192.168.255.0/255.255.255.0		否	
304	net-test	192.168.5.1/255.255.255.0		是	

图 5.1 对象 – 网络对象列表

◆ **创建网络对象**

在网络对象列表的右上方，单击【新建】，进入创建网络对象的界面，如图 5.2 所示。



图 5.2 对象 – 创建网络对象

创建网络对象时，各项参数含义如下：

编号——系统自动分配的网络对象编号，不能修改。

名称——必须填写网络对象名称，不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

IP 地址——网络对象的 IP 地址。

掩码——网络对象的子网掩码。

取反——选择**是**，表示将指定 IP 以外的 IP 地址作为该网络对象。

备注——填写备注信息，用来简单描述该网络对象。

◆ **编辑网络对象**

在网络对象列表的“配置”一栏中，单击图标即可编辑对应的网络对象（不能编辑系统缺省的 any 对象和正在使用中的 TAP 对象）。

◆ **删除网络对象**

在网络对象列表的“配置”一栏中，单击图标确认后即可删除对应的网络对象（不能删除系统缺省的 any 对象和正在使用中的网络对象）。

若要取消某个网络对象被使用的状态，可能需要进行以下操作：

1. 在网络组对象中，去掉该对象的选用，详细操作方法请参见 5.1.1.5 网络组对象；
2. 在防火墙规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.3 防火墙策略；
3. 在流量管理规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.6 流量管理策略；

4. 在入侵防护规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.5 入侵防护策略；
5. 在 IM/P2P 规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.7 IM/P2P 策略；
6. 在 WEB 安全规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.8 WEB 安全策略；
7. 在防病毒规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.9 防病毒策略；

5.1.1.2 节点对象

这里的节点是指单个 IP，即根据 IP 来指定的 IP 主机对象。

如图 5.3 所示，列出当前所有节点对象。对于无法删除的节点对象，表示已包含在网络组对象中或者正被某些规则使用，无论规则是否启用。

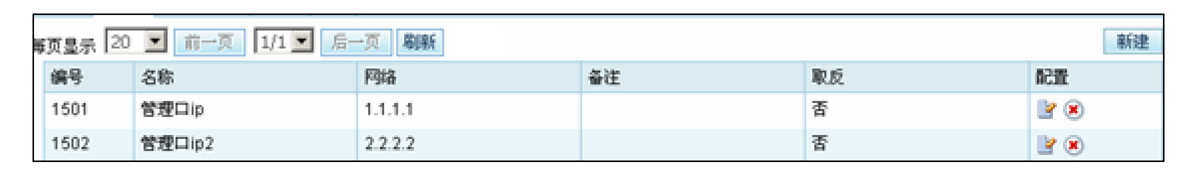


图 5.3 对象 – 节点对象列表

◆ **创建节点对象**

在节点对象列表的右上方，单击【新建】，进入创建节点对象的界面，如图 5.4 所示。



图 5.4 对象 – 创建节点对象

创建节点对象时，各项参数含义如下：

编号——系统自动分配的节点对象编号，不能修改。

名称——必须填写节点对象名称，不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

IP 地址——节点对象的单个 IP 地址。

取反——选择**是**，表示将指定 IP 以外的 IP 地址作为该节点对象。

备注——填写备注信息，用来简单描述该节点对象。

◆ **编辑节点对象**

在节点对象列表的“配置”一栏中，单击图标即可编辑对应的节点对象。

◆ **删除节点对象**

在节点对象列表的“配置”一栏中，单击图标确认后即可删除对应的节点对象（不能删除正在使用中的节点对象）。

若要取消某个节点对象被使用的状态，可能需要进行以下操作：

1. 在网络组对象中，去掉该对象的选用，详细操作方法请参见 5.1.1.5 网络组对象；
2. 在防火墙规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.3 防火墙策略；
3. 在流量管理规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.6 流量管理策略；
4. 在入侵防护规则中，取消源/目的对象包含该节点对象的规则的使用状态，详细操作方法请参见 5.5 入侵防护策略；
5. 在 IM/P2P 规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.7 IM/P2P 策略；
6. 在 WEB 安全规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.8 WEB 安全策略；
7. 在防病毒规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.9 防病毒策略；
8. 在一一映射或端口映射中，去掉内部/外部对象中对该对象的选用，详细操作方法请参见 4.2.1 静态路由部署。

5.1.1.3 MAC 地址对象

这里的 MAC 地址是为系统的防火墙策略配置而设计。在这里创建 MAC 地址对象后，配置防火墙策略时，用户可以引用此 MAC 地址，从而实现基于 MAC 的防火墙控制功能。

如图 5.5 所示，列出当前所有 MAC 地址对象。对于无法删除的 MAC 地址对象，表示已包含在网络组对象中或者正被某些规则使用，无论规则是否启用。

每页显示 20 前一页 1/1 后一页 刷新 新建 新建

编号	名称	MAC	备注	配置	配置
301	any	00:00:B4:00:01:0E			

图 5.5 对象 –MAC 地址对象列表

◆ **创建 MAC 地址对象**

在 MAC 地址对象列表的右上方，单击【新建】，进入创建 MAC 地址对象的界面，如图 5.6 所示。

新建

编号 3001

名称

MAC

备注

确定 取消

图 5.6 对象 – 创建 MAC 地址对象

创建 MAC 地址对象时，各项参数含义如下：

编号——系统自动分配的 MAC 地址对象编号，不能修改。

名称——必须填写 MAC 地址对象名称，不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

MAC 地址——MAC 对象的单个 MAC 地址。

备注——填写备注信息，用来简单描述该网络对象。

◆ **编辑 MAC 地址对象**

在 MAC 地址对象列表的“配置”一栏中，单击图标即可编辑对应的 MAC 地址对象（不能编辑正在使用中的 MAC 地址对象）。

◆ **删除 MAC 地址对象**

在 MAC 地址对象列表的“配置”一栏中，单击图标确认后即可删除对应的 MAC 地址对象（不能删除正在使用中的 MAC 地址对象）。

5.1.1.4 IP 池对象

IP 池是指一段连续的 IP，即从起始 IP 地址到结束 IP 地址之间的若干 IP 主机对象。

如图 5.7 所示，列出当前所有 IP 池对象。对于无法删除的 IP 池对象，表示已包含在网络组对象中或者正被某些规则使用，无论规则是否启用。

每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	网络	备注	取反	配置
1	NAT使用地址	200.200.200.4 - 200.200.200.5		否	
2	test-1	192.168.1.1 - 192.168.1.240		是	
3	test-2	192.168.11.1 - 192.168.11.5		否	

图 5.7 对象 – IP 池对象列表

◆ 创建 IP 池对象

在 IP 池对象列表的右上方，单击【新建】，进入创建 IP 池对象的界面，如图 5.8 所示。

编号 2
名称
开始地址
结束地址
取反 ○是 ⊙否
备注
确定 取消

图 5.8 对象 – 创建 IP 池对象

创建 IP 池对象时，各项参数含义如下：

编号——系统自动分配的 IP 池对象编号，不能修改。

名称——必须填写 IP 池对象名称，不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

开始地址/结束地址——IP 池对象的起始 IP 地址和结束 IP 地址，由此组成一个 IP 地址范围。

取反——选择**是**，表示将指定 IP 范围以外的 IP 地址作为该 IP 池对象。

备注——填写备注信息，用来简单描述该 IP 池对象。

◆ 编辑 IP 池对象

在 IP 池对象列表的“配置”一栏中，单击图标即可编辑对应的 IP 池对象。

◆ 删除 IP 池对象

在 IP 池对象列表的“配置”一栏中，单击图标确认后即可删除对应的 IP 池对象（不能删除正在使用中的 IP 池对象）。

若要取消某个 IP 池对象被使用的状态，可能需要进行以下操作：

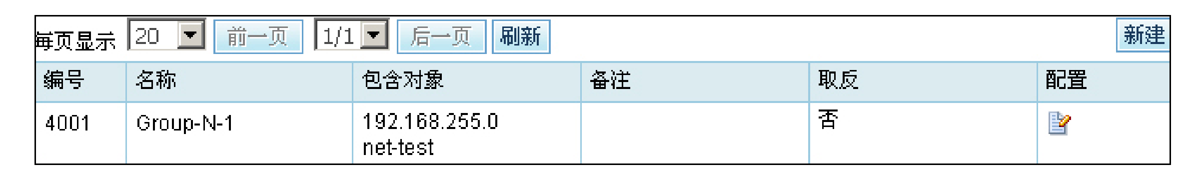
1. 在网络组对象中，去掉该对象的选用，详细操作方法请参见 5.1.1.5 网络组对象；

2. 在防火墙规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.3 防火墙策略；
3. 在流量管理规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.6 流量管理策略；
4. 在入侵防护规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.5 入侵防护策略；
5. 在 IM/P2P 规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.7 IM/P2P 策略；
6. 在 WEB 安全规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.8WEB 安全策略；
7. 在防病毒规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.9 防病毒策略；

5.1.1.5 网络组对象

这里的组是指若干个网络、节点或 IP 池对象组成的逻辑集合，组同样也可以包含其他组。

如图 5.9 所示，列出当前所有网络组对象。对于无法删除的网络组对象，表示已包含在其他网络组对象中或者正被某些规则使用，无论规则是否启用。



每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	包含对象	备注	取反	配置
4001	Group-N-1	192.168.255.0 net-test		否	

图 5.9 对象 – 网络组对象列表

◆ **创建网络组对象**

在网络组对象列表的右上方，单击【新建】，进入创建网络组对象的界面，如图 5.10 所示。



图 5.10 对象 – 创建网络组对象

创建网络组对象时，各项参数含义如下：

编号——系统自动分配的网络组对象编号，不能修改。

名称——必须填写网络组对象名称，不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

包含对象——单击框内任意位置，选择该网络组对象包含的网络对象（可以多选）。

取反——选择**是**，表示将指定对象以外的 IP 地址作为该网络组对象。

备注——填写备注信息，用来简单描述该网络组对象。

◆ **编辑网络组对象**

在网络组对象列表的“配置”一栏中，单击图标即可编辑对应的网络组对象。

◆ **删除网络组对象**

在网络组对象列表的“配置”一栏中，单击图标确认后即可删除对应的网络组对象（不能删除正在使用中的网络组对象）。

若要取消某个网络组对象被使用的状态，可能需要进行以下操作：

1. 在网络组对象的其他组对象中，去掉该对象的选用；
2. 在防火墙规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.3 防火墙策略；
3. 在流量管理规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.6 流量管理策略；
4. 在入侵防护规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.5 入侵防护策略；
5. 在 IM/P2P 规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.7 IM/P2P 策略；
6. 在 WEB 安全规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.8 WEB 安全策略；

7. 在防病毒规则中，去掉源/目的对象中对该对象的选用，详细操作方法请参见 5.9 防病毒策略；

5.1.2 服务对象

在设置策略路由、防火墙策略、流量管理策略时，需要引用服务对象来定义规则，分为以下三类服务对象：系统服务、自定义服务和服务组。

选择菜单【对象】➔【服务】，进入服务对象的设置页面。通过单击页面首部的标签，可以切换到相应的服务对象列表。

5.1.2.1 系统服务对象

系统服务对象，即系统预定义的服务对象，支持协议自识别和非固定端口的协议识别，包括常见的 ftp、bittorrent 等协议。如图 5.11 所示，列出出厂时已经设置的服务对象。

每页显示 10 前一页 1/10 后一页 刷新

编号	名称	协议	选项	备注
5001	any	any	null	Default
5002	echo[t]	tcp	源端口:any ; 目的端口:7	
5003	discard[t]	tcp	源端口:any ; 目的端口:9	
5004	discard[u]	udp	源端口:any ; 目的端口:9	
5005	systat[t]	tcp	源端口:any ; 目的端口:11	
5006	systat[u]	udp	源端口:any ; 目的端口:11	
5007	daytime[t]	tcp	源端口:any ; 目的端口:13	
5008	daytime[u]	udp	源端口:any ; 目的端口:13	
5009	ftp[t]	tcp	源端口:any ; 目的端口:21	FTP. control
5010	ssh[t]	tcp	源端口:any ; 目的端口:22	SSH Remote Login Protocol
5011	telnet[t]	tcp	源端口:any ; 目的端口:23	

图 5.11 对象 – 系统服务对象列表

 系统服务对象为系统自带的，不能编辑或删除，它会随着版本升级而有所变动。

5.1.2.2 自定义服务对象

除了系统服务对象，用户可以自定义服务对象，即自定义服务端口。

如图 5.12 所示，列出用户自定义的所有服务对象。对于无法删除的自定义服务对象，表示已包含在服务组对象中或者正被策略路由/防火墙/流量管理规则使用，无论规则是否启用。

每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	协议	选项	备注	配置
5601	自定义TCP	tcp	源端口:0-3388,3390-65535；目的端口:0-65535		
5602	自定义UDP	udp	源端口:0-65535；目的端口:21		
5603	自定义ICMP	icmp	type:1；code:2		
5604	自定义IP	ip	IP协议类型:88		

图 5.12　对象 – 自定义服务对象列表

◆　**创建自定义服务对象**

在自定义服务对象列表的右上方，单击【新建】，进入创建自定义服务对象的界面，如图 5.13 所示。

编号 5601
协议 TCP
名称
源端口 0-65535
目的端口 0-65535
备注
确定 取消

图 5.13　对象 – 创建自定义服务对象

创建自定义服务对象时，各项参数含义如下：

编号——系统自动分配的自定义服务对象编号，不能修改。

协议——选择一个协议类型，不同的类型对应不同的参数设置，例如：选择 **TCP** 或 **UDP** 协议则需要设置源/目的端口；选择 **ICMP** 协议则需要设置 type 和 code；选择 **IP** 协议则需要设置 IP 协议类型。

名称——必须填写自定义服务对象名称，不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

源端口——该服务对象使用的源端口，可以指定多个端口或端口范围，填写范围是 0-65535（仅当选择 **TCP** 或 **UDP** 协议时，设置此项）。

目的端口——该服务对象使用的目的端口，可以指定多个端口或端口范围，填写范围是 0-65535（仅当选择 **TCP** 或 **UDP** 协议时，设置此项）。

type——该服务对象的类型（仅当选择 **ICMP** 协议时，设置此项）。

code——该服务对象的代码（仅当选择 **ICMP** 协议时，设置此项）。

IP 协议类型——仅当选择 **IP** 协议时，设置此项。

备注——填写备注信息，用来简单描述该自定义服务对象。

◆ **编辑自定义服务对象**

在自定义服务对象列表的“配置”一栏中，单击图标即可编辑对应的服务对象。

◆ **删除自定义服务对象**

在自定义服务对象列表的“配置”一栏中，单击图标确认后即可删除对应的服务对象（不能删除正在使用中的自定义服务对象）。

若要取消某个自定义服务对象被使用的状态，可能需要进行以下操作：

1. 在服务组对象中，去掉该对象的选用，详细操作方法请参见 5.1.2.3 服务组对象；
2. 在防火墙规则中，去掉服务对象中对该对象的选用，详细操作方法请参见 5.3 防火墙策略；
3. 在流量管理规则中，去掉服务对象中对该对象的选用，详细操作方法请参见 5.6 流量管理策略；
4. 在策略路由规则中，去掉服务对象中对该对象的选用，详细操作方法请参见 5.2.3 策略路由。

5.1.2.3 服务组对象

这里的组是指若干系统服务对象和自定义服务对象组成的逻辑集合，组同样也可以包含其他组。

如图 5.14 所示，列出当前所有服务组对象。对于无法删除的服务组对象，表示已包含在其他服务组对象中或者正被策略路由/防火墙/流量管理规则使用，无论规则是否启用。

每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	包含对象	备注	配置
5801	Group-S-1	http[t] 自定义TCP 自定义IP		
5802	Group-S-2	ms-sql-s[t] ms-sql-s[u] ms-sql-m[t] ms-sql-m[u]		
5803	Group-S-3	自定义ICMP Group-S-2		

图 5.14 对象 – 服务组对象列表

◆ **创建服务组对象**

在服务组对象列表的右上方，单击【新建】，进入创建服务组对象的界面。创建方法与创建网络组对象的基本相同，详情请参见 5.1.1.5 网络组对象。

◆ **编辑服务组对象**

在服务组对象列表的“配置”一栏中，单击图标即可编辑对应的服务组对象。

◆ **删除服务组对象**

在服务组对象列表的“配置”一栏中，单击图标确认后即可删除对应的服务组对象（不能删除正在使用中的服务组对象）。

若要取消某个服务组对象被使用的状态，可能需要进行以下操作：

1. 在服务组对象的其他组对象中，去掉该对象的选用，详细方法请参见 5.1.2.3 服务组对象；
2. 在防火墙规则中，去掉服务对象中对该对象的选用，详细操作方法请参见 5.3 防火墙策略；
3. 在流量管理规则中，去掉服务对象中对该对象的选用，详细操作方法请参见 5.6 流量管理策略；
4. 在策略路由规则中，去掉服务对象中对该对象的选用，详细操作方法请参见 5.2.3 策略路由。

5.1.3 事件对象

在设置入侵防护策略时，需要选择事件对象来定义规则，分为以下三类事件对象：系统事件、自定义事件和事件组。

选择菜单【对象】➔【事件】，进入事件对象的设置页面。通过单击页面首部的标签，可以切换到相应的事件对象列表。

5.1.3.1 系统分组对象

系统分组对象，即系统预定义的由入侵防护规则库的多条规则组成的事件对象，并分类列出，如图 5.15 所示，其中 any 是系统缺省的事件对象，系统事件对象列表中其他分类的事件对象是 any 的一部分。

每页显示 10 前一页 1/5 后一页 刷新

编号	名称	所属大类	备注	配置
8001	any	-	Default	
8002	拒绝服务类攻击事件	攻击手段		
8003	获取权限类攻击事件	攻击手段		
8004	信息收集类攻击事件	攻击手段		
8005	可疑网络活动类事件	攻击手段		
8006	网络监控类功能事件	攻击手段		
8007	蠕虫事件	技术手段		
8009	病毒事件	技术手段		
8010	攻击事件	技术手段		
8011	普通事件	技术手段		
8012	非常流行事件	流行程度		

图 5.15 对象 – 系统分组对象列表

◆ **编辑系统分组对象**

在系统分组对象列表的“配置”一栏中，单击图标即可编辑对应的事件对象，如图 5.16 所示。

选中要使用的规则，表示使用该规则进行检测，符合此规则的网络行为都能被系统检测出来。编辑完毕请单击【确定】。

> 若要查看每条规则的具体内容，可直接单击规则 ID 或名称，系统会弹出规则的详细内容。此外，也可以在帮助页面执行搜索查看，具体操作方法请参见十一. NSFOCUS NIPS 规则库。

是否使用	事件
☑	[10142]3Com 3CDaemon TFTP保留设备名拒绝服务攻击
☑	[10146]Solaris Telnet服务远程Ctrl-D字符拒绝服务攻击
☑	[20417]Serv-U FTP服务器LIST命令超长-l参数远程拒绝服务攻击
☑	[10090]Artisoft XtraMail远程拒绝服务攻击
☑	[10098]Windows NT IIS/4.0 FTP NLST命令远程拒绝服务攻击
☑	[10152]H.225协议destinationAddress email-ID数据畸形
☑	[10153]H.225协议sourceAddress序列数据畸形
☑	[10150]Q.931协议Calling Party Number Length数据畸形
☑	[10151]H.225协议DestinationAddress序列数据畸形
☑	[10156]H.225协议Destination AliasAddress e164Number数据畸形
☑	[10157]H.225协议DestinationAddress H323-ID数据畸形

全部选择/取消

确定 取消

图 5.16 对象 – 编辑系统分组对象

⚠ 改变规则的使用属性后，需要手工执行【系统】➔【系统控制】➔【重启引擎】才能够生效。具体操作方法和注意事项请参见 9.7 系统控制。

◆ **搜索/定位系统分组对象**

系统分组对象的数量比较多，为了方便查找，可使用浏览器【编辑】➔【查找】或者使用快捷键 Ctrl+F 进行定位。

⚠ 系统分组对象为系统自带的，不能删除，它会随着版本升级而有所变动。

5.1.3.2 自定义规则

自定义规则，是指添加针对各种网络协议的自定义规则，即对系统自带的规则库的补充。

如图 5.17 所示，列出所有用户自定义的规则。对于无法删除的自定义规则，表示该规则已包含在自定义分组对象中。自定义规则的默认状态是不使用，若使规则生效必须将其状态设置为“使用”。

每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	类型	配置	是否使用
80001	自定义规则-IP	IP		
80002	自定义规则-UDP	UDP		
80003	自定义规则-TCP	TCP		
80004	自定义规则-ICMP	ICMP		
80005	自定义规则-HTTP	HTTP		
80006	自定义规则-POP3	POP3		
80007	自定义规则-SMTP	SMTP		
80008	自定义规则-MSN	MSN		
80009	自定义规则-QQTCP	QQ		
80010	自定义规则-QQUDP	QQ		
80011	自定义规则-FTP	FTP		

图 5.17 对象 – 自定义规则列表

若要取消某个自定义规则被包含的状态，需要在自定义分组对象中，去掉该对象的选择，详细操作方法请参见 5.1.3.3 自定义分组对象。

◆ **自定义 IP 规则**

新建一个自定义 IP 规则，协议类型设为 **IP**，如图 5.18 所示。

编号 80001
名称
级别 低风险事件
协议类型 IP
类型
包长度
关键字
确定 取消

图 5.18 对象 – 自定义 IP 规则

自定义 IP 规则的部分参数含义如下：

编号——系统自动分配的自定义规则对象编号，不能修改。

名称——自定义规则的显示名称。不能和已有规则重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

级别——选择该对象的风险级别。

类型——不同的协议类型，在此设置相应的参数（例如：TCP 类型填写 6，UDP 类型填写 17）。

包长度——如果协议号为 6，即 TCP 协议，其包长度为 **20+数据包 data 部分的长度**；如果协议号为 17，即 UDP 协议，其包长度为 **8+数据包 data 部分的长度**。

关键字——数据包 data 部分包含的内容。

关键字支持正则表达式，并且在默认情况下大小写不敏感，若以“case_”开头表示区分大小写。例如：填写 *case_WINDOWS*，只有 *WINDOWS* 能匹配，而 *Windows* 则不匹配。若不以“case_”开头则不区分大小写。

◆ **自定义 UDP 规则**

新建一个自定义 UDP 规则，协议类型设为 **UDP**，如图 5.19 所示。

编号	80002
名称	
级别	低风险事件
协议类型	UDP
源端口	
目的端口	
包长度	
关键字	
	确定 取消

图 5.19 对象 – 自定义 UDP 规则

自定义 UDP 规则的部分参数含义如下：

编号——系统自动分配的自定义规则对象编号，不能修改。

名称——自定义规则的显示名称。不能和已有规则重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

级别——选择该对象的风险级别。

源端口——UDP 包的源端口。

目的端口——UDP 包的目的端口。

包长度——数据包中 data 部分的长度。

关键字——数据包 data 部分包含的内容。

关键字支持正则表达式，并且在默认情况下大小写不敏感，若以“case_”开头表示区分大小写。例如：填写 *case_WINDOWS*，只有 *WINDOWS* 能匹配，而 *Windows* 则不匹配。若不以“case_”开头则不区分大小写。

◆ **自定义 TCP 规则**

自定义 TCP 规则的方法，与 UDP 规则的相同。

◆ **自定义 ICMP 规则**

新建一个自定义 ICMP 规则，协议类型设为 **ICMP**，如图 5.20 所示。

编号	80004
名称	
级别	低风险事件
协议类型	ICMP
类型	
包长度	
关键字	
	确定 取消

图 5.20 对象 – 自定义 ICMP 规则

自定义 ICMP 规则的部分参数含义如下：

编号——系统自动分配的自定义规则对象编号，不能修改。

名称——自定义规则的显示名称。不能和已有规则重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

级别——选择该对象的风险级别。

类型——差错或查询类型值。例如：查询的 ping 应答类型是 8，而差错的网络不可达错误类型是 3。

包长度——包长度是 **4+数据包 data 部分的长度**。例如：ping 2.2.2.2 –l 1，即 icmp data 长度是 1 字节，则包长度是 4+1=5。

关键字——数据包 data 部分包含的内容。

关键字支持正则表达式，并且在默认情况下大小写不敏感，若以“case_”开头表示区分大小写。例如：填写 *case_WINDOWS*，只有 *WINDOWS* 能匹配，而 *Windows* 则不匹配。若不以“case_”开头则不区分大小写。

◆ **自定义 HTTP 规则**

新建一个自定义 HTTP 规则，协议类型设为 **HTTP**，如图 5.21 所示。

编号	80005
名称	
级别	低风险事件
协议类型	HTTP
HTTP类型	POST
URL	
HOST	
关键字	
	确定 取消

图 5.21 对象 – 自定义 HTTP 规则

自定义 HTTP 规则的部分参数含义如下：

编号——系统自动分配的自定义规则对象编号，不能修改。

名称——自定义规则的显示名称。不能和已有规则重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

级别——选择该对象的风险级别。

HTTP 类型——选择 **POST**，表示发送出去的数据；选择 **GET**，表示接收到的数据。

URL/HOST——例如：www.google.com/index.htm，那么 www.google.com 属于 HOST，/index.htm 属于 URL。

关键字——网页内容中包含的关键字。目前不支持对 gzip 网页内容（关键字）的检测。

关键字支持正则表达式，并且在默认情况下大小写不敏感，若以“case_”开头表示区分大小写。例如：填写 *case_WINDOWS*，只有 *WINDOWS* 能匹配，而 *Windows* 则不匹配。若不以“case_”开头则不区分大小写。

◆ **自定义 POP3 规则**

新建一个自定义 POP3 规则，协议类型设为 **POP3**，如图 5.22 所示。

编号	80006
名称	
级别	低风险事件
协议类型	POP3
发件人	
收件人	
关键字	
	确定 取消

图 5.22 对象 – 自定义 POP3 规则

自定义 POP3 规则的部分参数含义如下：

编号——系统自动分配的自定义规则对象编号，不能修改。

名称——自定义规则的显示名称。不能和已有规则重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

级别——选择该对象的风险级别。

发件人——发件人的电子邮箱地址或地址中包含的内容。

收件人——收件人的电子邮箱地址或地址中包含的内容。

关键字——邮件正文内容中包含的关键字。

发件人、收件人和关键字均支持正则表达式，并且在默认情况下大小写不敏感，若以“case_”开头表示区分大小写。例如：填写 *case_WINDOWS*，只有 *WINDOWS* 能匹配，而 *Windows* 则不匹配。若不以“case_”开头则不区分大小写。

◆ **自定义 SMTP 规则**

自定义 SMTP 规则的方法，与 POP3 规则的相同。

◆ **自定义 MSN 规则**

新建一个自定义 MSN 规则，协议类型设为 **MSN**，如图 5.23 所示。



图 5.23 对象 – 自定义 MSN 规则

自定义 MSN 规则的部分参数含义如下：

编号——系统自动分配的自定义规则对象编号，不能修改。

名称——自定义规则的显示名称。不能和已有规则重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

级别——选择该对象的风险级别。

类型——选择**发送消息**，表示发送出去的 MSN 消息；选择**接收消息**，表示接收到的 MSN 消息。

关键字——MSN 消息正文中包含的关键字。

关键字支持正则表达式，并且在默认情况下大小写不敏感，若以“case_”开头表示区分大小写。例如：填写 *case_WINDOWS*，只有 *WINDOWS* 能匹配，而 *Windows* 则不匹配。若不以“case_”开头则不区分大小写。

◆ **自定义 QQTCP 规则**

新建一个自定义 QQTCP 规则，协议类型设为 **QQTCP**，如图 5.24 所示。



图 5.24 对象 – 自定义 QQTCP 规则

自定义 QQTCP 规则的部分参数含义如下：

编号——系统自动分配的自定义规则对象编号，不能修改。

名称——自定义规则的显示名称。不能和已有规则重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

级别——选择该对象的风险级别。

QQ 号——完整的 QQ 号码。

◆ **自定义 QQUDP 规则**

自定义 QQUDP 规则的方法，与 QQTCP 规则的相同。

◆ **自定义 FTP 规则**

新建一个自定义 FTP 规则，协议类型设为 **FTP**，如图 5.25 所示。

编号	80011
名称	
级别	低风险事件
协议类型	FTP
用户名	
文件名	
	确定 取消

图 5.25 对象 – 自定义 FTP 规则

自定义 FTP 规则的部分参数含义如下：

编号——系统自动分配的自定义规则对象编号，不能修改。

名称——自定义规则的显示名称。不能和已有规则重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

级别——选择该对象的风险级别。

用户名——ftp 服务访问帐号的用户名。

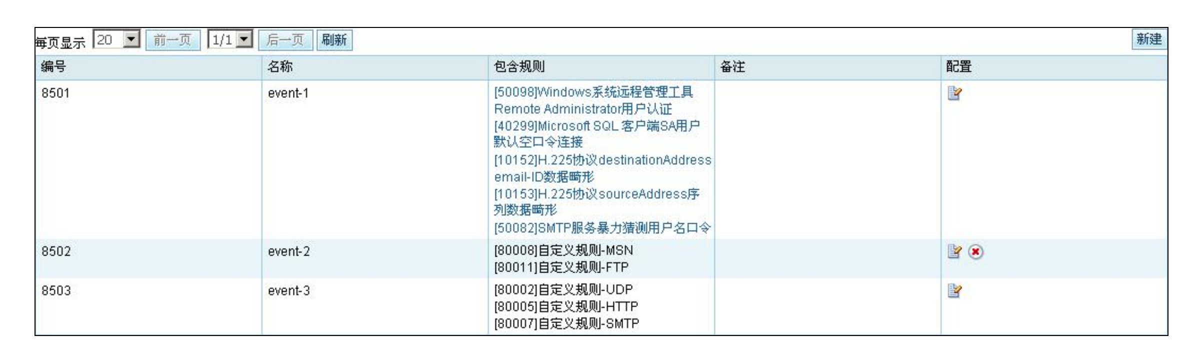
文件名——用户操作的文件名称。

用户名和文件名均支持正则表达式，并且在默认情况下大小写不敏感，若以“case_”开头表示区分大小写。例如：填写 *case_WINDOWS*，只有 *WINDOWS* 能匹配，而 *Windows* 则不匹配。若不以“case_”开头则不区分大小写。

5.1.3.3 自定义分组对象

自定义规则必须被选入自定义分组中，才能被入侵防护规则使用。用户可以自定义分组对象，即设置不同的规则集合。

如图 5.26 所示，列出用户自定义的所有分组对象。对于无法删除的自定义分组对象，表示该对象已包含在事件组对象中或者正被入侵防护规则使用，无论规则是否启用。


每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	包含规则	备注	配置
8501	event-1	[50098]Windows系统远程管理工具Remote Administrator用户认证 [40299]Microsoft SQL 客户端SA用户默认空口令连接 [10152]H.225协议destinationAddress email-ID数据畸形 [10153]H.225协议sourceAddress序列数据畸形 [50082]SMTP服务暴力猜测用户名口令		
8502	event-2	[80008]自定义规则-MSN [80011]自定义规则-FTP		
8503	event-3	[80002]自定义规则-UDP [80005]自定义规则-HTTP [80007]自定义规则-SMTP		

图 5.26 对象 – 自定义分组对象列表

◆ **创建自定义分组对象**

在自定义分组对象列表的右上方，单击【新建】，进入创建自定义分组对象的界面，如图 5.27 所示。


编号 8501
名称
备注
包含规则 攻击手段
⊞ 获取权限类攻击事件 全选/取消
⊞ 信息收集类攻击事件 全选/取消
⊞ 可疑网络活动类事件 全选/取消
⊞ 拒绝服务类攻击事件 全选/取消
⊞ 网络监控类功能事件 全选/取消
确定 取消

图 5.27 对象 – 创建自定义分组对象

创建自定义分组对象时，各项参数含义如下：

编号——系统自动分配的自定义分组对象编号，不能修改。

名称——必须填写自定义分组对象名称，不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

备注——填写备注信息，用来简单描述该自定义分组对象。

包含规则——先根据攻击手段、技术手段、流行程度、危险程度或服务类型选择规则类别，再据此选择该分组对象包含的入侵防护规则库规则（可以多选）。若要选择自定义规则，可以根据危险程度进行选择。

◆ **编辑自定义分组对象**

在自定义分组对象列表的“配置”一栏中，单击图标即可编辑对应的自定义分组对象。

◆ **删除自定义分组对象**

在自定义分组对象列表的“配置”一栏中，单击图标确认后即可删除对应的自定义分组对象（不能删除正在使用中的自定义分组对象）。

若要取消某个自定义分组对象被使用的状态，可能需要进行以下操作：

1. 在事件组对象中，去掉该对象的选用，详细操作方法请参见 5.1.3.4 事件组对象；

2. 在入侵防护规则中，去掉事件对象中对该对象的选用，详细操作方法请参见 5.5 入侵防护策略。

5.1.3.4 事件组对象

这里的组是指若干系统事件对象和自定义事件对象组成的逻辑集合，组同样也可以包含其他组。

如图 5.28 所示，列出当前所有的事件组对象。对于无法删除的事件组对象，表示已包含在其他事件组对象中或者正被入侵防护规则使用，无论规则是否启用。

每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	包含对象	备注	配置
9501	Group-E-1	蠕虫事件 病毒事件 event-3		
9502	Group-E-2	FTP事件 Telnet事件 event-1		
9503	Group-E-3	SQL事件 Group-E-2		

图 5.28 对象 – 事件组对象列表

◆ **创建事件组对象**

在事件组对象列表的右上方，单击【新建】，进入创建事件组对象的界面。创建方法与创建网络组对象的基本相同，详情请参见 5.1.1.5 网络组对象。

◆ **编辑事件组对象**

在事件组对象列表的“配置”一栏中，单击图标即可编辑对应的事件组对象。

◆ **删除事件组对象**

在事件组对象列表的“配置”一栏中，单击图标确认后即可删除对应的事件组对象（不能删除正在使用中的事件组对象）。

若要取消某个事件组对象被使用的状态，可能需要进行以下操作：

1. 在事件组对象的其他组对象中，去掉该对象的选用；
2. 在入侵防护规则中，去掉事件对象中对该对象的选用，详细操作方法请参见 5.5 入侵防护策略。

5.1.4 IM/P2P 对象

在设置 IM/P2P 策略时，需要选择 IM/P2P 对象来定义规则，分为以下四类 IM/P2P 对象：系统 IM/P2P、自定义 IM/P2P 规则、自定义 IM/P2P 分组和 IM/P2P 组。

选择菜单【对象】➔【IM/P2P】，进入 IM/P2P 对象的设置页面。通过单击页面首部的标签，可以切换到相应的 IM/P2P 对象列表。

5.1.4.1 系统对象

系统 IM/P2P 对象，即系统预定义的 IM/P2P 对象，包括常见的 IM 事件和 P2P 事件。如图 5.29 所示，列出出厂时已经设置的 IM/P2P 对象。

每页显示 20 前一页 1/1 后一页 刷新

编号	事件	备注	配置
28501	any	Default	
28502	股票软件		
28503	迅雷		
28504	BT下载		
28505	电驴		
28506	网际快车		
28507	网络游戏		
28509	益智休闲		
28510	即时通信软件		
28511	在线视频		
28512	全部游戏	包含网络游戏，益智游戏等	
28513	全部P2P下载	包括电驴、BT、迅雷等	

图 5.29 对象 – 系统 IM/P2P 对象列表

 系统 IM/P2P 对象为系统自带的，不能删除，它会随着版本升级而有所变动。

5.1.4.2 自定义规则

自定义 IM/P2P 规则与自定义事件规则基本一致，详情请参见 5.1.3.2 自定义规则。

5.1.4.3 自定义分组对象

除了系统 IM/P2P 对象，用户可以自定义 IM/P2P 对象。

如图 5.30 所示，列出用户自定义的所有 IM/P2P 对象。对于无法删除的自定义 IM/P2P 对象，表示已包含在 IM/P2P 组对象中或者正被 IM/P2P 规则使用，无论规则是否启用。



每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	包含规则	备注	配置
28601	自定义-P2P-1	[50077]P2P文件共享工具BitTorrent获取文件信息 [50071]P2P文件共享工具eDonkey/ed2k连接服务器 [50073]P2P文件共享工具eDonkey/ed2k请求文件片断(TCP) [50072]P2P文件共享工具eDonkey/ed2k搜索文件		
28602	自定义-IM-1	[50086]即时通信软件MSN发现非法信息 [50087]即时通信软件MSN发现传送可疑文件 [50124]即时通信软件ICQ用户发送可疑文件 [50125]即时通信软件ICQ发现非法信息		
28603	自定义-P2P-2	[50254]HTTP协议多线程文件下载 [50255]网络未知加密数据传输 [50256]飞鸽传输数据通信		

图 5.30 对象 – 自定义 IM/P2P 对象列表

◆ **创建自定义 IM/P2P 对象**

在自定义 IM/P2P 对象列表的右上方，单击【新建】，进入创建自定义 IM/P2P 对象的界面，如图 5.31 所示。

新建

编号 28601

名称

包含规则

- [50099]网络游戏平台中国游戏中心登录
- [50251]P2P软件TeamViewer文件下载
- [50250]P2P软件FS2YOU文件下载
- [50252]P2P软件FlashGet文件下载
- [50075]即时通信软件MSN Messenger用户登录
- [50074]即时通信软件ICQ用户登录
- [50077]P2P文件共享工具BitTorrent获取文件信息
- [50071]P2P文件共享工具eDonkey/ed2k连接服务器
- [50073]P2P文件共享工具eDonkey/ed2k请求文件片断(TCP)
- [50072]P2P文件共享工具eDonkey/ed2k搜索文件
- [50079]网络游戏星际争霸（Starcraft）客户端连接服务器
- [50078]网络游戏反恐精英（CS）客户端连接服务器

备注

确定 取消

图 5.31 对象 – 创建自定义 IM/P2P 对象

创建自定义 IM/P2P 对象时，各项参数含义如下：

编号——系统自动分配的自定义 IM/P2P 对象编号，不能修改。

名称——必须填写自定义 IM/P2P 对象名称，不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

包含规则——选择该对象包含的 IM/P2P 规则（可以多选）。

备注——填写备注信息，用来简单描述该自定义 IM/P2P 对象。

◆ **编辑自定义 IM/P2P 对象**

在自定义 IM/P2P 对象列表的“配置”一栏中，单击图标即可编辑对应的 IM/P2P 对象。

◆ **删除自定义 IM/P2P 对象**

在自定义 IM/P2P 对象列表的“配置”一栏中，单击图标确认后即可删除对应的 IM/P2P 对象（不能删除正在使用中的自定义 IM/P2P 对象）。

若要取消某个自定义 IM/P2P 对象被使用的状态，可能需要进行以下操作：

1. 在 IM/P2P 组对象中，去掉该对象的选择，详细操作方法请参见 5.1.4.4 IM/P2P 组对象；
2. 在 IM/P2P 策略中，去掉事件对象中对该对象的选用，详细操作方法请参见 5.7 IM/P2P 策略。

5.1.4.4 IM/P2P 组对象

这里的组对象是指若干系统 IM/P2P 对象和自定义 IM/P2P 对象组成的逻辑集合，组同样也可以包含其他组。

如图 5.32 所示，列出当前所有的 IM/P2P 组对象。对于无法删除的 IM/P2P 组对象，表示已包含在其他 IM/P2P 组对象中或者正被 IM/P2P 规则使用（无论规则是否启用）。



每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	包含对象	备注	配置
28701	Group-P-1	迅雷 BT下载 电驴		
28702	Group-IM-1	即时通信软件 自定义IM-1		
28703	Group-P-2	全部游戏 全部P2P下载 Group-P-1		

图 5.32 对象 – IM/P2P 组对象列表

◆ **新建 IM/P2P 组对象**

在 IM/P2P 组对象列表的右上方，单击【新建】，进入创建 IM/P2P 组对象的界面。创建方法与创建网络组对象的基本相同，详情请参见 5.1.1.5 网络组对象。

◆ **编辑 IM/P2P 组对象**

在 IM/P2P 组对象列表的“配置”一栏中，单击图标即可编辑对应的 IM/P2P 组对象。

◆ **删除 IM/P2P 组对象**

在 IM/P2P 组对象列表的“配置”一栏中，单击图标确认后即可删除对应的 IM/P2P 组对象（不能删除正在使用中的 IM/P2P 组对象）。

若要取消某个自定义 IM/P2P 对象组被使用的状态，可能需要进行以下操作：

1. 在 IM/P2P 组对象的其他组对象中，去掉该对象的选用；
2. 在 IM/P2P 策略中，去掉事件对象中对该对象的选用，详细操作方法请参见 5.7IM/P2P 策略。

5.1.5 时间对象

在设置所有策略时，均需选择时间对象来定义规则，分为以下两类时间对象：自定义时间和时间组。

选择菜单【对象】➔【时间】，进入时间对象的设置页面。通过单击页面首部的标签，可以切换到相应的时间对象列表。

5.1.5.1 自定义时间对象

每个时间对象都可包含两个时间段，用户可以根据具体情况来自定义时间对象。

如图 5.33 所示，列出当前所有自定义时间对象，其中 any 是系统缺省的时间对象。对于无法删除的自定义时间对象，表示该对象已包含在时间组对象中或者正被某些规则使用，无论规则是否启用。



每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	类型	时间	备注	配置
6001	any	每天	00:00 - 23:59 ; 00:00 - 23:59	Default	
6002	morning	每天	00:00 - 11:59 ; 00:00 - 00:00		
6003	noon	每天	13:00 - 17:59 ; 00:00 - 00:00		
6004	night	每个工作日	18:00 - 23:59 ; 00:00 - 00:00		
6005	meeting	每月	日期 : 1,28 时间 : 00:00 - 23:59 ; 00:00 - 00:00		
6006	week	每周	周日 : 00:00 - 17:59 ; 00:00 - 00:00 周一 : 09:00 - 17:59 ; 00:00 - 00:00 周二 : 09:00 - 17:59 ; 00:00 - 00:00 周三 : 09:00 - 17:59 ; 00:00 - 00:00 周四 : 09:00 - 17:59 ; 00:00 - 00:00 周五 : 09:00 - 17:59 ; 00:00 - 00:00 周六 : 00:00 - 23:59 ; 00:00 - 00:00		

图 5.33 对象 – 自定义时间对象列表

◆ **创建自定义时间对象**

在自定义时间对象列表的右上方，单击【新建】，进入创建自定义时间对象的界面，如图 5.34 所示。



图 5.34 对象 – 创建自定义时间对象

创建自定义时间对象时，各项参数含义如下：

编号——系统自动分配的自定义时间对象编号，不能修改。

类型——分为**每天**、**每个工作日**、**每周**和**每月**四类，其中每个工作日表示每周一至周五。

名称——必须填写自定义时间对象名称，不能和已有对象重名，且不能使用非法字符（非法字符包括/%\{}`@^<>'&":和空格）。

时间——时间对象可以包含两个时间段，如果只需定义一个时间段，只需将第二个时间段都保持为系统默认的 00:00 即可。对于**每月**，还需设置具体日期（填写方式请参见界面帮助）。

备注——填写备注信息，用来简单描述该自定义时间对象。

◆ **编辑自定义时间对象**

在自定义时间对象列表的“配置”一栏中，单击图标即可编辑对应的时间对象（不能编辑系统缺省的 any 对象）。

◆ **删除自定义时间对象**

在自定义时间对象列表的“配置”一栏中，单击图标确认后即可删除对应的时间对象（不能删除系统缺省的 any 对象和正在使用中的自定义时间对象）。

若要取消某个自定义时间对象被使用的状态，可能需要进行以下操作：

1. 在时间组对象中，去掉该对象的选用，详细操作方法请参见 5.1.5.2 时间组对象；
2. 在防火墙规则中，去掉时间对象中对该对象的选用，详细操作方法请参见 5.3 防火墙策略；
3. 在流量管理规则中，去掉时间对象中对该对象的选用，详细操作方法请参见 5.6 流量管理策略；
4. 在入侵防护规则中，去掉时间对象中对该对象的选用，详细操作方法请参见 5.5 入侵防护策略；
5. 在 IM/P2P 规则中，去掉时间对象中对该对象的选用，详细操作方法请参见 5.7IM/P2P 策略；
6. 在 WEB 安全规则中，去掉时间对象中对该对象的选用，详细操作方法请参见 5.8WEB 安全策略；
7. 在防病毒规则中，去掉时间对象中对该对象的选用，详细操作方法请参见 5.9 防病毒策略；

5.1.5.2 时间组对象

这里的组是指若干自定义时间对象组成的逻辑集合，组同样也可以包含其他组。

如图 5.35 所示，列出当前所有的时间组对象。对于无法删除的时间组对象，表示已包含在其他时间组对象中或者正被某些规则使用，无论规则是否启用。



编号	名称	包含对象	备注	配置
6301	Group-T-1	morning meeting		
6302	Group-T-2	morning noon		
6303	Group-T-3	week Group-T-1		

图 5.35 对象 – 时间组对象列表

◆ **创建时间组对象**

在时间组对象列表的右上方，单击【新建】，进入创建时间组对象的界面。创建方法与创建网络组对象的基本相同，详情请参见 5.1.1.5 网络组对象。

◆ **编辑时间组对象**

在时间组对象列表的“配置”一栏中，单击图标即可编辑对应的时间组对象。

◆ **删除时间组对象**

在时间组对象列表的“配置”一栏中，单击图标确认后即可删除对应的时间组对象（不能删除正在使用中的时间组对象）。

若要取消某个时间组对象被使用的状态，可能需要进行以下操作：

1. 在时间组对象的其他组对象中，去掉该对象的选用；
2. 在防火墙规则中，去掉时间对象中对该对象的选用，详细操作方法请参见 5.3 防火墙策略；
3. 在流量管理规则中，去掉时间对象中对该对象的选用，详细操作方法请参见 5.6 流量管理策略；
4. 在入侵防护规则中，去掉时间对象中对该对象的选用，详细操作方法请参见 5.5 入侵防护策略；
5. 在 IM/P2P 规则中，去掉时间对象中对该对象的选用，详细操作方法请参见 5.7IM/P2P 策略；
6. 在 WEB 安全规则中，去掉时间对象中对该对象的选用，详细操作方法请参见 5.8 WEB 安全策略；
7. 在防病毒规则中，去掉时间对象中对该对象的选用，详细操作方法请参见 5.9 防病毒策略；

5.2 路由

网络路由包括三部分：静态路由、动态路由和策略路由。其中，静态路由和策略路由是在 Web 管理界面中进行配置，动态路由是在串口管理菜单中进行配置。

5.2.1 静态路由

选择菜单【网络】➔【路由】➔【静态路由】，进入网络路由的设置页面。

静态路由是在 NSFOCUS NIPS 引擎中设置的一组固定的路由表，除非手工指定，否则不会发生变化。静态路由根据目标 IP 及其网络掩码来对 IP 分组进行路由。

如图 5.36 所示，列出当前所有静态路由的信息，管理员可以对其进行配置。



图 5.36 路由 – 静态路由列表

◆ **创建静态路由**

在静态路由列表的右上方，单击【新建】，进入创建静态路由的界面，如图 5.37 所示。



图 5.37 路由 – 创建静态路由

创建静态路由时，各项参数含义如下：

编号——系统自动分配的静态路由编号，不能修改。

静态路由名称——不能包含/%\{}`@^<>'&":和空格等非法字符。

目标 IP 地址/网络掩码——目标主机的 IP 地址及其子网掩码。

网关地址——网关的 IP 地址，能够完成与目标主机的通讯。

接口——此静态路由出口的网络接口。

优先级——优先级范围是 1 至 30，数字越小表示级别越高。

◆ **编辑静态路由**

在静态路由列表的“配置”一栏中，单击图标即可编辑对应的静态路由信息。

◆ **删除静态路由**

在静态路由列表的“配置”一栏中，单击图标确认后即可将对应的静态路由删除。

5.2.2 动态路由

与 CISCO IOS 管理界面类似，通过串口或者 SSH 方式连接 NSFOCUS NIPS 的 50022 端口并登录（初始用户名和密码均是 shell，通过 SSH 方式需要打开远程协助），然后使用命令行的方式配置动态路由（与 CISCO 的 OSPF、RIP 和 BGP 命令的使用方法一致）。

有关串口的登录方法，请参见 10.2 登录串口。

5.2.3 策略路由

选择菜单【网络】➔【路由】➔【策略路由】，进入网络路由的设置页面。

策略路由是在 NSFOCUS NIPS 引擎中设置的另一组固定的路由表，除非手工指定，否则不会发生变化。策略路由根据源 IP 及其网络掩码、目标 IP 及其网络掩码和服务来对 IP 分组进行路由。

如图 5.38 所示，列出当前所有策略路由的信息，管理员可以对其进行配置。


每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	源IP	源网络掩码	目标IP	目标网络掩码	网关	协议	接口	优先级	配置
1	PolicyRouting-1	192.168.5.0	255.255.255.0	192.168.10.0	255.255.255.0	192.168.5.254	any	eth0	1	
2	PolicyRouting-2	192.168.6.0	255.255.255.0	192.168.12.0	255.255.255.0	192.168.6.254	TCP ftp[t]	eth4	3	

图 5.38 路由 – 策略路由列表

◆ **创建策略路由**

在策略路由列表的右上方，单击【新建】，进入创建策略路由的界面，如图 5.39 所示。


编号 1
策略路由名称
源IP地址
网络掩码
目标IP地址
网络掩码
网关地址
服务对象 any
接口 eth0
优先级
确定 取消

图 5.39 路由 – 创建策略路由

创建策略路由时，各项参数含义如下：

编号——系统自动分配的策略路由编号，不能修改。

策略路由名称——不能使用非法字符。

源 IP 地址/网络掩码——源主机的 IP 地址及其子网掩码。

目标 IP 地址/网络掩码——目标主机的 IP 地址及其子网掩码。

网关地址——网关的 IP 地址，能够完成与目标主机的通讯。

服务对象——此策略路由使用的服务对象（有关服务对象的设置方法，请参见 5.1.2 服务对象）。

接口——此策略路由出口的网络接口，只有在三层转发（Layer3）或管理（Mgt）模式下才能设置策略路由。

优先级——优先级范围是 1~30，数字越小表示级别越高。

◆ **编辑策略路由**

在策略路由列表的“配置”一栏中，单击图标即可编辑对应的策略路由信息。

◆ **删除策略路由**

在策略路由列表的“配置”一栏中，单击图标确认后即可将对应的策略路由删除。

路由配置（包括静态路由和策略路由）变更（增加、删除或修改）后，需要手工执行【系统】➔【系统控制】➔【重启引擎】才能够生效。具体操作方法和注意事项请参见 9.7 系统控制。

系统优先匹配动态路由，然后再匹配策略路由，最后匹配静态路由。

5.3 防火墙策略

选择菜单【策略】➔【防火墙】，进入防火墙策略配置的页面，可以进行防火墙规则的添加、编辑、删除、复制和上下移动等操作。若要查看防火墙规则的“动作”或“选项”，可以将鼠标置于对应的图标上，即可显示提示信息。对于出现红叉的编号，表示该规则没有使用。

防火墙默认允许一切通讯。

5.3.1 阻断功能

使用防火墙策略的阻断功能之前，需要先确认源安全区到目的安全区的信息通过何种协议进行阻断。

以单路部署方式为例，阻断 IRC 的 TCP 协议连接的配置方法如下：

（1）创建一条防火墙规则，如图 5.40 所示。

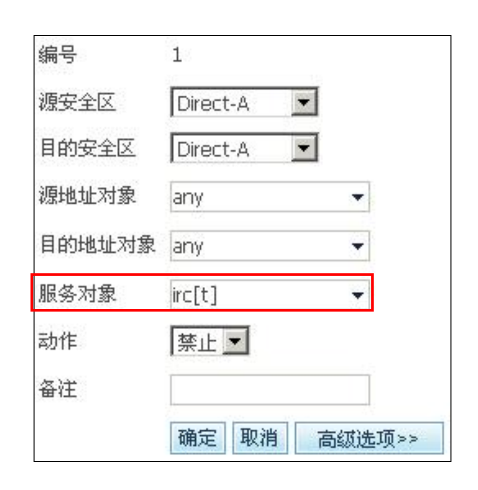


图 5.40 防火墙策略 – 设置阻断功能

（2）确定后返回防火墙规则列表，如图 5.41 所示。



Direct-A/Direct-A:共1条

编号	源对象	目的对象	服务	动作	选项	使用	配置
1	any	any	TCP irc[t]			☑	

图 5.41 防火墙策略 – 设置阻断功能的规则

5.3.2 认证功能

5.3.2.1 认证配置

在配置防火墙规则时，若要将动作设置为“认证”的前提是客户端已经安装并开启绿盟内网安全管理系统的代理端软件（以下简称 NSFOCUS EPS）或者启用了 Ldap 认证功能、Radius 认证功能、本地认证功能的其中一项并正常通过认证，这样数据包才能通过 NSFOCUS NIPS，否则会阻断该客户端的通讯。

选择菜单【策略】➔【防火墙】➔【认证配置】，即可进行防火墙认证的各项参数配置，各项参数配置完毕，单击【确定】，如图 5.42 所示。

认证设置	
Ldap认证	○开启 ◉关闭
认证服务器	0.0.0.0
认证持续时间(秒)	3600
Radius认证	○开启 ◉关闭
认证服务器	0.0.0.0
认证方式	chap
认证端口	1812
认证共享密钥	●●●
认证持续时间(秒)	3600
本地认证	○开启 ◉关闭
认证持续时间(秒)	3600
EPS联动	○开启 ◉关闭
EPS服务器地址	0.0.0.0
本地联动端口	8080
配置信息	
认证重定向地址	0.0.0.0
	确定

图 5.42　防火墙策略 – 认证配置

防火墙认证配置的主要参数含义如下：

Ldap 认证——选择**开启**，表示开启 Ldap 认证服务，并在下面设置 Ldap 认证服务器的 IP 地址和认证持续时间（单位：秒）。

Radius 认证——选择**开启**，表示开启 Radius 认证服务，并在下面设置 Radius 认证服务器的 IP 地址、认证方式、认证端口、认证共享密钥和认证持续时间（单位：秒）。

本地认证——选择**开启**，表示开启本地认证服务，并在下面设置本地认证的持续时间（单位：秒）。

EPS 联动开关——选择**开启**，表示开启 NSFOCUS NIPS 与 NSFOCUS EPS 的联动功能，并在下面设置 NSFOCUS EPS 服务器的 IP 地址和本地联动端口。

认证重定向地址——NSFOCUS NIPS 设备管理口的 IP 地址，并且在客户端访问网络时，该地址必须可达。

开启认证开关之后（例如：EPS 联动开关），需要在防火墙策略中添加动作为“认证”的规则才能够配合实现相关控制，具体操作方法请参见 5.3.2.2 添加规则。如需了解 NSFOCUS EPS 产品的详细功能，请联系绿盟科技的技术支持人员。

开启本地认证之前，需导入本地用户认证库，具体导入方法请参见 9.1.2 导入升级文件。

5.3.2.2 添加规则

正确配置防火墙策略的各项认证参数之后，必须在防火墙策略中添加相应规则，才能使认证功能生效。下面举例说明防火墙规则的配置方法：

例如：必须在安装 NSFOCUS EPS 的代理端软件之后，才允许从内网访问外网。配置方法如下：

（1）创建一条防火墙规则，如图 5.43 所示。



图 5.43 防火墙策略 – 设置 NSFOCUS EPS 认证功能

（2）确定后返回防火墙规则列表，如图 5.44 所示。



Intranet/Extranet:共1条

编号	源对象	目的对象	服务	动作	选项	使用	配置
1	any	any	any				

图 5.44 防火墙策略 – 设置 NSFOCUS EPS 认证功能的规则

（3）选择菜单【策略】➔【防火墙】➔【认证配置】，开启 EPS 联动开关并进行相关配置。假设 NSFOCUS EPS 服务器的 IP 地址是 192.168.1.25，端口是 60001，它必须与 NSFOCUS NIPS 的内网接口保持正常通讯，才能保证联动生效。

5.3.3 NAT 功能

从内网访问外网时，内网是私有 IP 地址，需要使用 NAT 功能转换为公网 IP 地址才能访问。

例如：转换后的公网 IP 地址是 222.222.222.222，配置方法如下：

（1）选择菜单【对象】➔【网络】➔【节点】，创建 NAT 地址对象，如图 5.45 所示。



图 5.45 防火墙策略 – 设置 NAT 地址对象

（2）配置从内网访问外网的防火墙规则，如图 5.46 所示。



图 5.46 防火墙策略 – 设置防火墙规则（NAT 功能）

当 NAT 地址对象的 IP 地址更改后，需要重启引擎，配置才能生效。

配置 NAT 规则时，同一 NAT 地址对象不能用于多条规则，否则会引起网络异常。

5.3.4 一一映射和端口映射

5.3.4.1 一一映射

一一映射是将 DMZ 区域的某个服务器完全映射到公网，所有端口全部开放，如果从内网通过域名访问该服务器，必须同时选中“同步修改 DNS 指向”。

例如：内网服务器 IP 地址是 1.1.1.1，映射到公网的 IP 地址是 2.2.2.2。配置方法如下：

（1）选择菜单【网络】➔【接口】，编辑连接 DMZ 区域的接口的一一映射规则，如图 5.47 所示。



图 5.47 一一映射 – 设置接口的一一映射规则

（2）设置完毕，返回连接 DMZ 区域的接口的一一映射规则列表，如图 5.48 所示。

是否使用	编号	内部对象	外部对象	选项	备注	配置
☑	2	1.1.1.1	2.2.2.2	REF dns		

图 5.48 一一映射 – 设置完毕的一一映射规则列表

一一映射的配置需要重启引擎才能生效。

5.3.4.2 端口映射

端口映射是将 DMZ 区域的某个服务器的某个端口映射到公网（本地端口和向外映射的端口不必完全一致），只需保持映射的端口是开放状态。如果从内网通过域名访问该服务器，可以同时选中“同步修改 DNS 指向”。

端口映射支持一对多和多对多的映射，通过负载均衡，提高服务器响应速度。

例如：内网服务器 IP 地址是 1.1.1.1，内部使用 8080 端口，映射到公网的 IP 地址是 2.2.2.2，外部端口是 80。配置方法如下：

（1）选择菜单【网络】➔【接口】➔【端口映射】，编辑连接 DMZ 区域的接口的端口映射规则，如图 5.49 所示。



图 5.49 端口映射 – 设置接口的端口映射规则

（2）设置完毕，返回连接 DMZ 区域的接口的端口映射规则列表，如图 5.50 所示。

是否使用	编号	内部对象	内部端口	外部对象	外部端口	协议	选项	备注	配置
☑	2	1.1.1.1	8080	2.2.2.2	80	tcp	REF dns		

图 5.50 端口映射 – 设置完毕的端口映射规则列表

⚠端口映射的配置需要重启引擎才能生效。

5.4 IDS 联动

NSFOCUS NIPS 在实现过程中提供了多种二次开发接口，可以使 NSFOCUS NIPS 与其他安全产品进行整合。例如：NSFOCUS NIPS 可以与 NSFOCUS NIDS 设备配合，对网络进行监控。

5.5 入侵防护策略

通过设置入侵防护策略，可以实现不同的入侵防护功能。

选择菜单【策略】➔【入侵防护】，进入入侵防护策略配置的页面，可以进行入侵防护规则的添加、编辑、删除、复制和上下移动等操作。若要查看入侵防护规则的“动作”或“选项”，可以将鼠标置于对应的图标上，即可显示提示信息。对于出现红叉的编号，表示该规则没有使用。

下面以单路 Direct 部署方式下，对蠕虫事件和病毒事件进行入侵防护为例，介绍入侵防护规则的配置方法（要求蠕虫和病毒全部阻断，检查其他所有事件）：

（1）配置阻断病毒和蠕虫的入侵防护规则，选择**病毒事件**和**蠕虫事件**对象，告警方式保持默认设置（默认是**安全中心显示**和**写入日志数据库**），阻断动作保持默认设置（默认是**阻断**），如图 5.51 所示。



图 5.51 入侵防护策略 – 创建阻断蠕虫和病毒的规则

（2）配置检查全部事件的入侵防护规则，如图 5.52 所示。告警方式保持默认设置（默认是**安全中心显示**和**写入日志数据库**），阻断动作选择**否**。



图 5.52　入侵防护策略 – 创建检查全部事件的规则

（3）全部配置完毕，返回入侵防护规则列表，如图 5.53 所示。



Direct-A/Direct-A:共1条

编号	源对象	目的对象	事件	动作	选项	使用	配置
1	any	any	蠕虫事件 病毒事件			☑	

global/any:共1条

编号	源对象	目的对象	事件	动作	选项	使用	配置
2	any	any	any			☑	

图 5.53　配置完毕的入侵防护规则列表

5.6 流量管理策略

通过流量管理策略，可以保证网络带宽合理使用，以及按照协议对流量进行限制或保障。

5.6.1 保证带宽

保证带宽，就是保障某种协议最小的使用带宽情况。例如：在 10M 网络环境中，需要保障 HTTP 协议 2M 的带宽，如图 5.54 所示。



图 5.54 流量管理策略 – 创建流量管理规则（保证带宽）

5.6.2 最大带宽

最大带宽，就是限制某种协议的最大带宽。例如：在 10M 网络环境中，需要限制 P2P 下载协议最多占用 1M 的带宽，如图 5.55 所示。

编号	2
源安全区	Intranet
目的安全区	Extranet
源对象	any
目的对象	any
时间	any
服务	p2p_bittorrent[t]
优先级	2
保证带宽(kbps)	0
最大带宽(kbps)	1000
最大会话数	0
每IP最大带宽(kbps)	0
每IP最大会话数	0
备注	
	确定 取消

图 5.55　流量管理策略 – 创建流量管理规则（最大带宽）

5.7 IM/P2P 策略

除了入侵防护策略，对于各类 IM/P2P 事件的检测，还可以自定义 IM/P2P 策略，以实现不同的检测/保护需求。

选择菜单【策略】➔【IM/P2P】，进入 IM/P2P 策略配置的页面，可以进行 IM/P2P 规则的添加、编辑、删除、复制和上下移动等操作。若要查看 IM/P2P 规则的"动作"或"选项"，可以将鼠标置于对应的图标上，即可显示提示信息。对于出现红叉的编号，表示该规则没有使用。

下面以单路 Direct 部署方式下，对 IM/P2P 事件进行检测/阻断为例，介绍 IM/P2P 规则的配置方法（要求迅雷、BT 下载和电驴全部阻断，在线视频和网络游戏事件上班时间阻断、下班后允许，检测其他所有事件）：

（1）配置阻断迅雷、BT 下载和电驴的规则，选择**迅雷**、**BT 下载**和**电驴**事件对象，告警方式保持默认设置（默认是**安全中心显示**和**写入日志数据库**），阻断动作保持默认设置（默认是**阻断**），如图 5.56 所示。



图 5.56 IM/P2P 策略 – 创建阻断迅雷、BT 下载和电驴的规则

（2）选择菜单【对象】➔【时间】，自定义上班时间对象，如图 5.57 所示。



图 5.57 IM/P2P 策略 – 定义上班时间对象

（3）上班时间对象设置完毕，返回自定义时间对象列表，如图 5.58 所示。



每页显示 20 前一页 1/1 后一页 刷新 新建

编号	名称	类型	时间	备注	配置
6001	any	每天	00:00 - 23:59 ; 00:00 - 23:59	Default	
6002	Work	每个工作日	09:00 - 12:00 ; 13:00 - 18:00		

图 5.58 IM/P2P 策略 – 时间对象列表

（4）配置在线视频和网络游戏事件上班时间的规则，如图 5.59 所示。告警方式保持默认设置（默认是**安全中心显示**和**写入日志数据库**），阻断动作保持默认设置（默认是**阻断**），时间对象选择 **Work**。

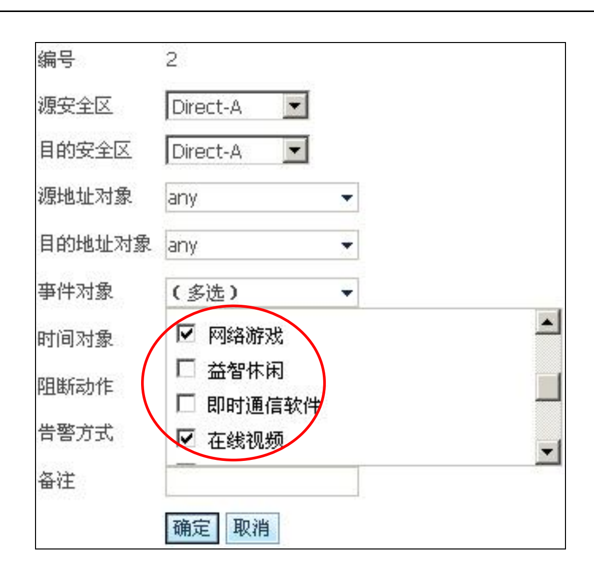


图 5.59 IM/P2P 策略 – 创建在线视频和网络游戏事件上班时间的规则

（5）配置检查全部事件的 IM/P2P 规则，如图 5.60 所示。告警方式保持默认设置（默认是**安全中心显示**和**写入日志数据库**），阻断动作选择**否**。



图 5.60 IM/P2P 策略 – 创建检查全部事件的规则

（6）全部配置完毕，返回 IM/P2P 规则列表，如图 5.61 所示。



Direct-A/Direct-A:共2条

编号	源对象	目的对象	事件	动作	选项	使用	配置
1	any	any	迅雷 BT下载 电驴				
2	any	any	网络游戏 在线视频				

global/any:共1条

编号	源对象	目的对象	事件	动作	选项	使用	配置
3	any	any	any				

图 5.61 配置完毕的 IM/P2P 规则列表

5.8 WEB 安全策略

WEB 安全策略主要是用来进行网站分类的审计和过滤，包括 Web 信誉和 URL 过滤。

5.8.1 WEB 信誉策略配置

选择菜单【策略】➔【WEB 安全】➔【WEB 信誉】，进入 WEB 信誉配置的页面，可以查看恶意库的当前版本信息以及功能配置如图 5.62 所示。

恶意库基本信息	
版本	5.6.0.11
最新更新时间	2009.03.16 16:13:08
恶意站点条数	298,538
配置信息	
web信誉	☑ 启用
是否允许跳过阻止页面	☑ 启用
	确定

图 5.62 WEB 安全策略 – 配置 Web 信誉

Web 信誉的配置信息如下：

Web 信誉——选中此项，表示开启了 WEB 安全策略的功能。

是否允许跳过阻止页面——只有启用了 Web 信誉，才能启用此项。选中此项，表示当 NSFOCUS NIPS 提示某网站为可疑站点时，用户可以选择继续访问该站点，如图 5.63 所示；否则，该站点会直接被阻断，用户无法访问。

潜在的威胁站点

提示您:此网页被标识为不适当的网页

地址:

如果您认为不应该阻止此网页，请单击此链接跳过

版权所有 © 2009 绿盟科技

图 5.63 WEB 安全策略 – 触发规则时的页面显示

5.8.2 URL 过滤策略配置

举例说明：需要过滤的网站类型包括色情和成人网站两类内容，针对它的 WEB 管理规则的配置方法如下：

（1）选择菜单【策略】➔【WEB 安全】➔【URL 过滤】，创建一条针对色情和成人网站阻断的规则，如图 5.64 所示。



图 5.64 WEB 安全策略 – 创建 URL 过滤规则

（2）配置完毕，返回 URL 过滤规则列表并启用该规则，如图 5.65 所示。



编号	源对象	目的对象	时间	分类	动作	使用	配置
1	any	any	any	色情 成人		☑	

图 5.65 配置完毕的 URL 过滤规则列表

5.9 防病毒策略

防病毒策略可以针对 HTTP（包括 Webmail）、SMTP、FTP 和 POP3 协议进行病毒检测。

5.9.1 启用防病毒引擎

配置防病毒策略前，需要开启防病毒功能。防病毒引擎包括两类：Nsfocus 防病毒引擎和 Kaspersky 防病毒引擎。二者既可以独立使用，也可以协同工作（开启病毒引擎之前，请确认已经成功导入病毒库升级包，具体导入方法请参见 9.1.2 导入升级文件）。

选择菜单【策略】➔【防病毒】➔【防病毒配置】，即可配置 Nsfocus 防病毒引擎和 Kaspersky 防病毒引擎。

1. 开启 Nsfocus 防病毒引擎

如图 5.66 所示，配置 Nsfocus 防病毒引擎中 HTTP、SMTP、FTP 和 POP3 协议的禁用内容以及最大解压层数，用来保证防病毒策略准确生效。

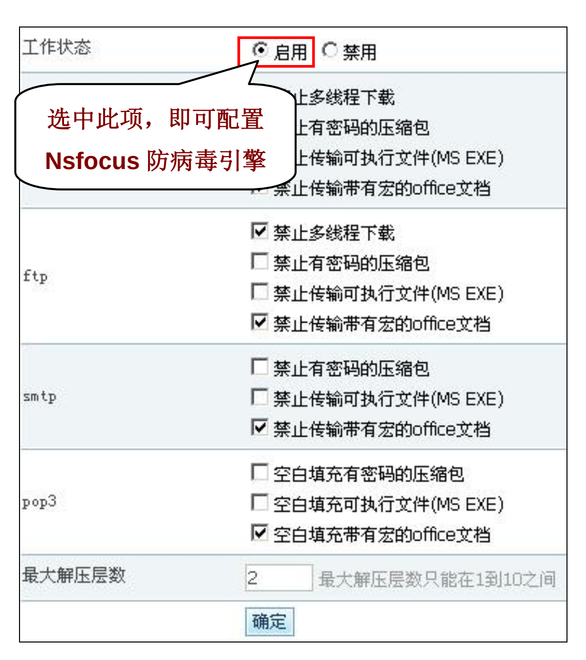


图 5.66 防病毒策略 – Nsfocus 病毒引擎配置

2. 开启 Kaspersky 防病毒引擎

开启 Kaspersky 防病毒引擎即可，无需配置具体选项。

若要启用 Kaspersky 病毒引擎，必须选择菜单【策略】➔【防病毒】➔【许可证】，导入 NSFOCUS NIPS 的 Kapspersky 证书文件（*.lic），导入之后引擎可能会自动重启。

5.9.2 防病毒策略配置

5.9.2.1 添加防病毒策略

防病毒引擎开启之后，需要添加防病毒规则。例如：只针对 HTTP、POP3 和 SMTP 协议的防病毒规则，配置方法如下：

（1）选择菜单【策略】➔【防病毒】➔【防病毒策略】，创建一条 HTTP、POP3 和 SMTP 协议的防病毒规则，如图 5.67 所示。告警方式保持默认设置（默认是**安全中心显示**和**写入日志数据库**），阻断动作保持默认设置（默认是**阻断**）



图 5.67 防病毒策略 – 创建防病毒规则

（2）配置完毕，返回防病毒规则列表并启用该规则，如图 5.68 所示。



每页显示 20 前一页 1/1 后一页 刷新 新建

global/any:共1条

编号	源对象	目的对象	时间	协议	使用	配置
1	any	any	any	http smtp pop3	☑	

图 5.68 配置完毕的防病毒规则列表

5.9.2.2 防病毒配置

系统有两类防病毒引擎：

- NSFOCUS 病毒引擎
- Kasperkay 病毒引擎

在防病毒配置界面，可以控制防病毒引擎的开启和关闭，并对部分参数进行配置。

◆ **NSFOCUS 病毒引擎的配置**

选择菜单【策略】➔【防病毒】➔【防病毒配置】➔【NSFOCUS 病毒引擎】，如图 5.69 所示。

NSFOCUS 病毒引擎默认为启用状态。

NSFOCUS病毒引擎	Kaspersky病毒引擎
工作状态	◉启用 ○禁用
http	☑禁止多线程下载 ☐禁止有密码的压缩包 ☐禁止传输可执行文件(MS EXE) ☑禁止传输带有宏的office文档
ftp	☑禁止多线程下载 ☐禁止有密码的压缩包 ☐禁止传输可执行文件(MS EXE) ☑禁止传输带有宏的office文档
smtp	☐禁止有密码的压缩包 ☐禁止传输可执行文件(MS EXE) ☑禁止传输带有宏的office文档
pop3	☐空白填充有密码的压缩包 ☐空白填充可执行文件(MS EXE) ☑空白填充带有宏的office文档
最大解压层数	1 最大解压层数只能在1到10之间
	确定

图 5.69 防病毒配置 – NSFOCUS 病毒引擎

◆ **Kasperkay 病毒引擎的配置**

选择菜单【策略】➔【防病毒】➔【防病毒配置】➔【Kasperkay 病毒引擎】，如图 5.70 所示。



图 5.70 防病毒配置 – Kasperkay 病毒引擎

Kasperkay 病毒引擎默认为禁用状态。在首次开启 Kasperkay 病毒引擎时，请先导入 Kasperkay 许可证，导入方法请参见 5.9.2.4 许可证。

5.9.2.3 设置白名单

若是不希望有些特殊文件通过病毒扫描引擎，需选择菜单【策略】➔【防病毒】➔【白名单】，将不需通过病毒扫描引擎的文件后缀名添加到白名单中，例如：*.txt* 或者*.jpg*，如图 5.71 所示。

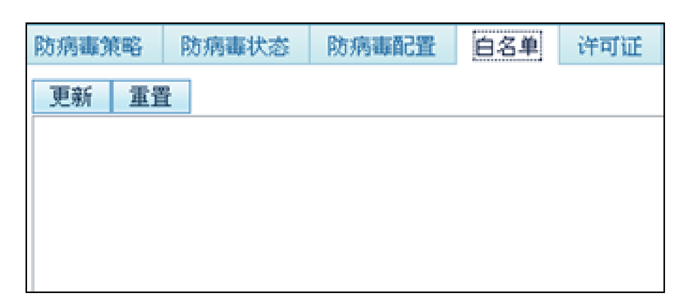


图 5.71 防病毒策略 – 白名单

5.9.2.4 许可证

选择菜单【策略】➔【防病毒】➔【许可证】，如图 5.72 所示。单击【浏览】，选择 Kasperkay 许可证路径，上传许可证。

⚠导入 Kasperkay 许可证时，系统可能会自动重启。



图 5.72 防病毒配置 – 许可证

5.9.2.5 防病毒病毒库状态

选择菜单【策略】➔【防病毒】➔【防病毒状态】，即可查看当前病毒库的版本信息，包括大版本号、小版本号、最新更新的时间和病毒库条目总数，如图 5.73 所示。

Nsfocus病毒库信息	
版本	5.6.1.55
最新更新时间	2009/02/24 12:08
病毒库条目总数	495,130
Kapspersky病毒库信息	
版本	5.6.1.13
最新更新时间	2009/02/24 12:03
病毒库条目总数	1,380,230

图 5.73 防病毒策略 – 病毒库版本信息

5.10 透明代理策略

透明代理是指客户端不必设置代理的参数就可使用代理，使客户端感觉不到代理的存在，便可完成内外网络的通讯。当内部用户需要使用透明代理访问外部资源时，用户不需要进行设置，代理服务器会建立透明的通道，让用户直接与外界通信，极大地方便了用户的使用。

⚠只有加载了防火墙模块，产品才有透明代理功能。

选择菜单【策略】➔【透明代理】，进入 WEB 透明代理配置的页面，即可新建不同对象的透明代理。比如新建一个透明代理使源地址对象为内网的用户通过 HTTP 访问外网，具体配置如图 5.74 所示。



图 5.74 透明代理－新建配置

⚠源安全区和目的安全区必须配置在三层安全区。

配置完毕，返回透明代理配置列表，如图 5.75 所示。



图 5.75 透明代理配置列表

5.11 DHCP 服务

DHCP 称为动态主机配置协议。NSFOCUS NIPS 的 DHCP 配置包括以下两部分的配置：

◆ **DHCP 服务**

DHCP 服务允许工作站连接到网络并自动获取一个 IP 地址。配置 DHCP 服务的服务器可以为每一个网络客户提供一个 IP 地址、子网掩码、缺省网关、一个 WINS 服务器的 IP 地址以及一个 DNS 服务器的 IP 地址。

◆ **DHCP 中继**

DHCP 中继（DHCP relay agent）能够把 DHCP/BOOTP 广播信息从一个网段转播到另一个网段上。

5.11.1 DHCP 服务配置

选择菜单【网络】➔【DHCP】➔【DHCP 服务】，进入 DHCP 服务的设置页面，初始状态下 DHCP 服务列表为空。

下面举例说明 DHCP 服务的设置方法：

1. 新建动态 DHCP 服务

DHCP 动态服务，即服务器接收到一个来自客户的 IP 租用请求时，它会根据自己的作用域地址池为该客户保留一个 IP 地址并且在网络上广播一个 DHCP Offer 封包，该消息包含客户的 MAC 地址、服务器提供的 IP 地址、子网掩码、租用期限以及租用的 DHCP 服务器本身的 IP 地址。

新建一个动态 DHCP 服务，如图 5.76 所示。

所属接口	eth0
名称	client-1
类型	动态
子网	192.168.10.0
起始IP	192.168.10.120
终止IP	192.168.10.150
网关	192.168.10.254
子网掩码	255.255.255.0
租约时间	36000
DNS服务器1	192.168.1.2
DNS服务器2	202.106.0.20
DNS服务器3	
WINS服务器1	192.168.1.1
WINS服务器2	

确定 取消 高级选项<<

图 5.76 DHCP – 新建动态 DHCP 服务

2. 新建静态 DHCP 服务

DHCP 静态服务，即服务器接收到一个来自客户的 IP 租用请求时，它会根据客户端的 MAC 地址信息，从 DHCP 服务中选取该 MAC 地址对应的 IP 地址、子网掩码、租用期限以及提供该租用的 DHCP 服务器本身的 IP 地址。

新建一个静态 DHCP 服务，如图 5.77 所示。



所属接口	eth1
名称	client-2
类型	静态
MAC地址	00-06-1B-DF-7D-13
主机名	client-2
IP地址	192.168.10.160
网关	192.168.10.254
子网掩码	255.255.255.0
租约时间	36000

确定 取消 高级选项>>

图 5.77 DHCP – 新建静态 DHCP 服务

3. 配置完毕的 DHCP 服务列表

动态 DHCP 服务和静态 DHCP 服务配置完毕，返回 DHCP 服务列表，如图 5.78 所示。



每页显示 20 | 前一页 | 1/1 | 后一页 | 刷新 | 新建

所属接口	名称	类型	是否使用	配置
eth0	client-1	动态	☑	
eth1	client-2	静态	☑	

图 5.78 DHCP – 配置完毕的 DHCP 服务列表

⚠ DHCP 服务器的工作接口的安全区类型必须是 mgt 类型。

5.11.2 DHCP 中继配置

选择菜单【网络】➔【DHCP】➔【DHCP 中继】，进入 DHCP 中继的设置页面。初始状态下 DHCP 中继列表为空。

下面举例说明 DHCP 中继的设置方法：

1. 新建 DHCP 中继

新建一个静态 DHCP 服务，如图 5.79 所示。



图 5.79 DHCP – 新建 DHCP 中继

DHCP 中继的各项参数含义如下：

源接口——接收 DHCP 请求的接口。

目的接口——DHCP 服务器可以应答的接口。

2. 配置完毕的 DHCP 中继列表

DHCP 中继配置完毕，返回 DHCP 中继列表，如图 5.80 所示。NSFOCUS NIPS 会将 eth2 接口获取的 DHCP 请求转发到 eth0 接口。另外，应答消息从 eth0 接口返回到 eth2 接口，实现 DHCP 中继。



每页显示 20 | 前一页 | 1/1 | 后一页 | 刷新 | 新建

源接口	目的接口	配置
eth2	eth0	

图 5.80 DHCP – 配置完毕的 DHCP 服务列表

5.11.3 租约列表

选择菜单【网络】➔【DHCP】➔【租约列表】，即可在此查看获取 DHCP 服务的客户端信息，如图 5.81 所示。

所属接口	IP地址	主机名	MAC地址	起始时间	结束时间
eth4	10.14.66.5	WWW-E38A8EDB4CF	00:22:B0:69:15:16	2009-04-09 13:09:25	2009-04-09 13:14:25

图 5.81 DHCP – 租约列表

5.12 DNS 服务

DNS 服务是互联网上非常重要和基础的服务之一，用来确定主机名和 IP 地址之间的对应关系。NSFOCUS NIPS 提供了 DNS 服务解析的功能。

5.12.1 DNS 服务器配置

选择菜单【网络】➔【DNS】➔【服务器】，进入 DNS 服务器的设置页面，初始状态下 DNS 服务器列表为空。

下面举例说明 DNS 服务器的设置方法：

1. 新建 DNS 服务器

新建一个 DNS 服务器，如图 5.82 所示。



图 5.82 DNS – 新建 DNS 服务器

2. 配置完毕的 DNS 服务器列表

DNS 服务器配置完毕，返回 DNS 服务器列表，如图 5.83 所示。对于 DNS 服务器列表以外的域名，系统将无法解析。


每页显示 20 前一页 1/1 后一页 刷新 新建

域名	IP地址	是否启用	配置
server1.intra.nsfocus.com	192.168.1.10	☑	

图 5.83 DNS – 配置完毕的 DNS 服务器列表

5.12.2 DNS 客户端配置

NSFOCUS NIPS 访问域名时，需要配置 DNS 客户端信息。

选择菜单【网络】➔【DNS】➔【客户端】，进入 DNS 客户端的设置页面，如图 5.84 所示。



图 5.84 DNS – 新建 DNS 客户端

DNS 客户端配置完毕，NSFOCUS NIPS 通过其他 DNS 服务器来解析域名，与 NSFOCUS NIPS 自身提供的 DNS 服务无关。

 DNS 服务器的工作接口的安全区类型必须是 mgt 类型。

5.13 IPMAC 绑定

通过 IP 地址和 MAC 地址的绑定，防止特定的客户端通过将主机 IP 修改为可以上网的网段，从而实现联网的目的。选择菜单【网络】➔【IPMAC 绑定】，进入 IPMAC 绑定的设置页面，如图 5.85 所示，列出所有被绑定的 IP 地址和 MAC 地址。

每页显示 20 前一页 1/1 后一页 刷新 导入 新建 全部删除

是否使用	编号	IP	MAC	备注	配置
☑	1	192.168.5.29	00:11:22:33:44:55		
☐	2	10.10.5.187	00:40:C1:2B:5C:29		
☑	3	10.10.5.217	00:31:48:23:68:5A		

图 5.85 网络 – IP 和 MAC 绑定规则列表

◆ **新建 IPMAC 绑定规则**

在 IP 和 MAC 绑定规则列表的右上方，单击【新建】，进入创建绑定 IP 地址和 MAC 地址的界面，如图 5.86 所示。

新建的 IPMAC 地址，不能与已有的 IP 或 MAC 地址重复。

新建的 IP 地址不能与 NSFOCUS NIPS 的网关 IP 地址重复。

编号 1

IP

MAC

备注

确定 取消

图 5.86 网络 – 新建 IP 地址与 MAC 地址的绑定

◆ **导入 IPMAC 绑定规则**

在 IP 和 MAC 绑定规则列表的右上方，单击【导入】，既可以通过浏览的方式导入文件，又可以通过手动填写的方式输入多个 IPMAC 地址。

导入 IPMAC 地址，不能与已有的 IP 或 MAC 地址重复。

NSFOCUS NIPS 的网关 IP 地址，不能被导入。

◆ **编辑 IPMAC 绑定规则**

在 IP 和 MAC 绑定规则列表的“配置”一栏中，单击图标即可编辑对应的绑定规则。

◆ **删除 IPMAC 绑定规则**

在 IP 和 MAC 绑定规则列表的“配置”一栏中，单击图标即可删除对应的绑定规则。

在 IP 和 MAC 绑定规则列表的右上方，单击【全部删除】，在弹出的确认对话框中单击【确认】，即可一次删除所有的绑定规则。

◆ **启用 IPMAC 绑定规则**

在 IP 和 MAC 绑定规则列表中，所有的规则默认是启用状态。若要取消启用状态，单击“使用”一栏下的选框，取消选中的状态。

◆ **导出 IPMAC 绑定规则**

选择菜单【网络】➔【IPMAC 绑定】➔【IPMAC 在线状态】，进入 IPMAC 在线状态查看界面，显示当前系统自学习到的 IPMAC 地址对应表，即对经过 NIPS 的数据包，系统可以自己学习到 IP 和 MAC 地址，如图 5.87 所示。单击图中按钮【导出】，可导出列表。

IPMAC 自学习功能仅在三层安全区下有效。

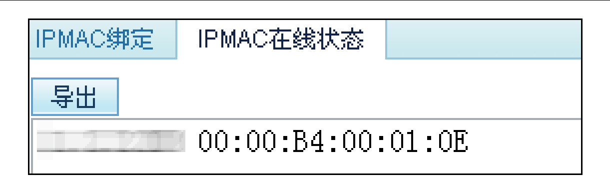


图 5.87　网络 – IPMAC 在线状态

5.14 策略配置生效方式

策略配置完毕，必须选择菜单【系统】➔【系统控制】➔【应用配置】才能生效。

有关系统控制的详细介绍，请参见 9.7 系统控制。

六. 查看实时事件

管理员可以在此查看 NSFOCUS NIPS 引擎的实时流量统计和最新的告警事件信息，其中告警事件包括四类：入侵防护事件、IM/P2P 事件、WEB 安全事件和防病毒事件。

6.1 流量

选择菜单【首页】➔【流量】，即可实时查看流量总体统计信息、排名前十位的 TCP 协议分布信息和 UDP 协议分布信息，如图 6.1 所示。

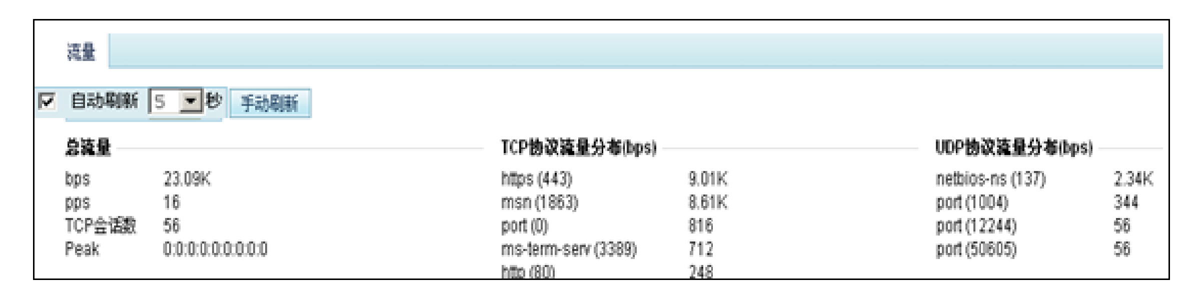


图 6.1 NSFOCUS NIPS 引擎实时流量统计信息

6.2 入侵防护事件

如图 6.2 所示，实时显示最近发生的 20 条入侵防护事件的状态、时间、事件内容和源/目的 IP 及其端口，亦可以事件详情的形式列出。刷新的方式有两种：自动刷新和手动刷新。

在状态一栏中，表示该事件在客户端的状态是允许（在入侵防护规则中，针对该事件的阻断动作为**否**）；表示该条事件在客户端的状态是阻断（在入侵防护规则中，针对该事件的阻断动作为**是**）。



图 6.2 事件 – 入侵防护事件 TOP20

6.3 IM/P2P 事件

如图 6.3 所示，实时显示最近发生的 20 条 IM/P2P 事件的状态、时间、事件内容和源/目的 IP 及其端口，亦可以事件详情的形式列出。刷新的方式有两种：自动刷新和手动刷新。

在状态一栏中，表示该事件在客户端的状态是允许（在 IM/P2P 规则中，针对该事件的阻断动作为否）；表示该条事件在客户端的状态是阻断（在 IM/P2P 规则中，针对该事件的阻断动作为是）。



时间	事件	源
-04 11:28:15	[50085]即时通信软件MSN用户接收消息	
-04 11:28:15	[50085]即时通信软件MSN用户接收消息	
-04 11:28:15	[50084]即时通信软件MSN用户发送消息	
2009-04-04 11:28:15	[50085]即时通信软件MSN用户接收消息	
2009-04-04 11:28:13	[50084]即时通信软件MSN用户发送消息	
2009-04-04 11:28:13	[50085]即时通信软件MSN用户接收消息	
2009-04-04 11:28:13	[50193]PPLive网络电视流媒体播放(UDP)	
2009-04-04 11:28:11	[50084]即时通信软件MSN用户发送消息	
2009-04-04 11:28:11	[50193]PPLive网络电视流媒体播放(UDP)	
2009-04-04 11:28:11	[50193]PPLive网络电视流媒体播放(UDP)	
2009-04-04 11:28:09	[50085]即时通信软件MSN用户接收消息	
2009-04-04 11:28:09	[50085]即时通信软件MSN用户接收消息	
2009-04-04 11:28:09	[50085]即时通信软件MSN用户接收消息	
2009-04-04 11:28:09	[50193]PPLive网络电视流媒体播放(UDP)	
2009-04-04 11:28:09	[50193]PPLive网络电视流媒体播放(UDP)	
2009-04-04 11:28:09	[50193]PPLive网络电视流媒体播放(UDP)	
2009-04-04 11:28:09	[50193]PPLive网络电视流媒体播放(UDP)	
2009-04-04 11:28:09	[50084]即时通信软件MSN用户发送消息	
2009-04-04 11:28:09	[50084]即时通信软件MSN用户发送消息	
2009-04-04 11:28:07	[50084]即时通信软件MSN用户发送消息	

图 6.3 事件 – IM/P2P 事件 TOP20

6.4 WEB 安全事件

如图 6.4 所示，实时显示最近发生的 20 条 WEB 安全事件的状态、时间、源/目的 IP 及其端口、事件类型和 URL 等。刷新的方式有两种：自动刷新和手动刷新。



时间	源	目的	分类	站点
4-04 11:48:09			财经证券	finance.sina.com.cn
4-04 11:48:07			新闻	news.sina.com.cn
4-04 11:48:07			新闻	news.sina.com.cn
2009-04-04 11:47:57			新闻	news.sohu.com
2009-04-04 11:47:07			malware	www.ggqjsj.net
2009-04-04 11:47:07			malware	www.ggqjsj.net
2009-04-04 11:47:07			malware	www.ggqjsj.net
2009-04-04 11:47:07			malware	www.kouchischool.com
2009-04-04 11:47:07			malware	www.ggqjsj.net
2009-04-04 11:47:07			malware	www.sg18.com
2009-04-04 11:47:07			malware	www.sg18.com
2009-04-04 11:47:07			malware	www.rzyx.com
2009-04-04 11:47:07			malware	www.rzyx.com
2009-04-04 11:47:06			malware	www.sg18.com
2009-04-04 11:47:06			malware	www.rzyx.com
2009-04-04 11:47:06			malware	www.rzyx.com
2009-04-04 11:47:04			malware	www.eecce.com
2009-04-04 11:47:04			malware	www.eecce.com
2009-04-04 11:47:04			malware	www.rzyx.com
2009-04-04 11:47:04			malware	www.rzyx.com

图 6.4 事件 – WEB 安全事件 TOP20

在 WEB 安全事件 TOP20 列表中，各项参数含义如下：

状态——表示该事件在客户端的状态是允许（在 WEB 安全规则中，针对该事件的阻断动作为否）；表示该条事件在客户端的状态是阻断（在 WEB 安全规则中，针对该事件的阻断动作为是）。

时间——WEB 安全事件发生的具体时间。

源/目的 IP 及其端口——WEB 安全事件发生的源/目的 IP 及其端口。

分类——WEB 安全事件的类型，包括 malware、求职招聘、web 邮件、色情和成人等。

站点——WEB 安全事件的 URL。

6.5 防病毒事件

如图 6.5 所示，实时显示最近发生的 20 条防病毒事件的状态、时间、事件内容和源/目的 IP 及其端口，亦可以事件详情的形式列出。刷新的方式有两种：自动刷新和手动刷新。

在状态一栏中，表示该事件在客户端的状态是允许（在防病毒规则中，针对该事件的阻断动作为否）；表示该条事件在客户端的状态是阻断（在防病毒规则中，针对该事件的阻断动作为是）。



图 6.5 事件 – 防病毒事件 TOP20

七. 日志分析

用户可以设置条件，对 NSFOCUS NIPS 的各类日志进行查询，包括防火墙日志、入侵防护日志、IM/P2P 日志、WEB 安全日志、防病毒日志和系统日志，还可以将查询结果导出或打印，以便于统计分析。

7.1 防火墙日志

通过查看防火墙日志，可以方便管理员排查 NAT 或防火墙问题，并进行调试。如图 7.1 所示，防火墙日志报表是按照数据库存储的，当数量超过 1 万条时，将删除一部分旧日志，开始新的日志记录。

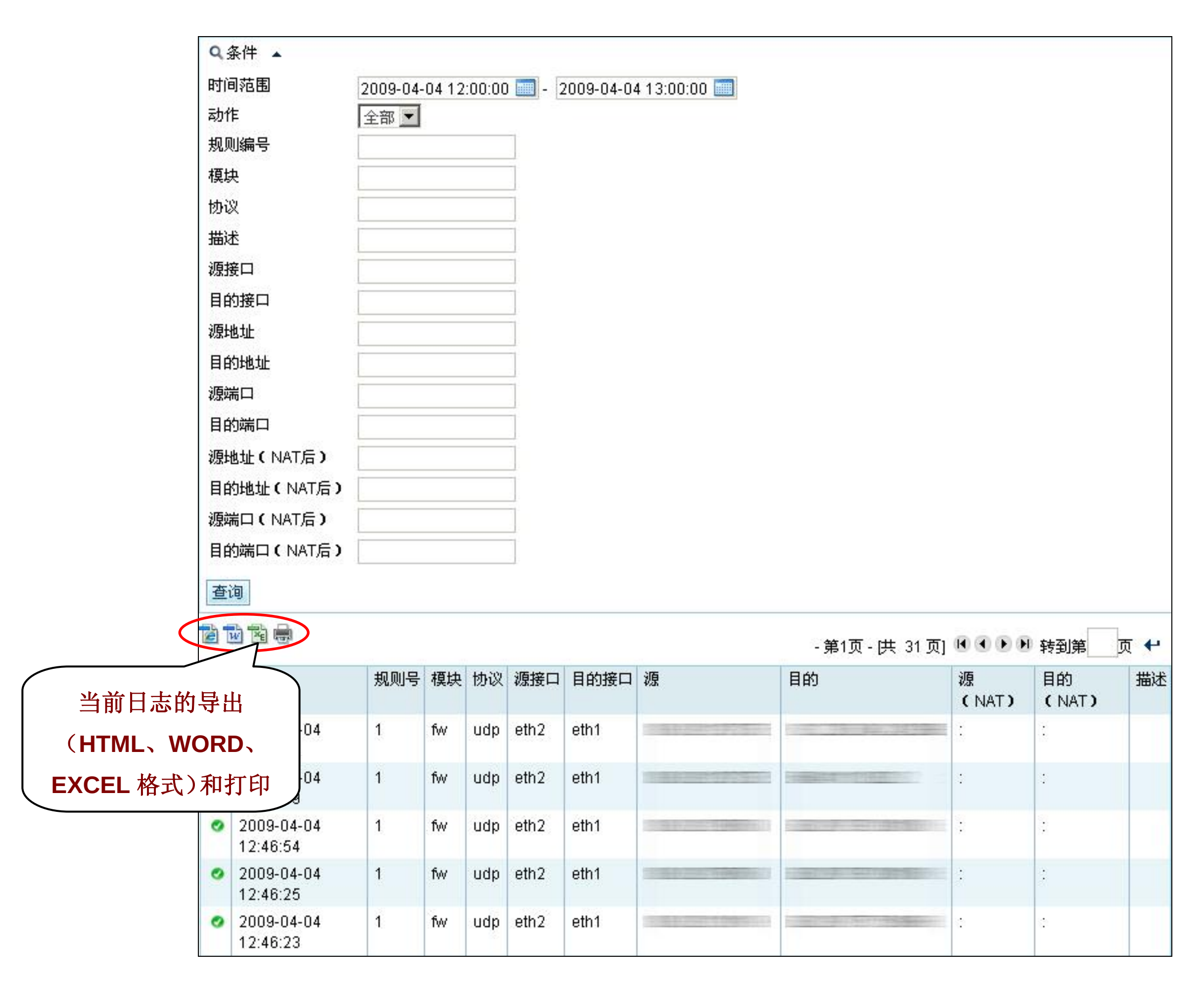


图 7.1 日志分析 – 防火墙日志

◆ 日志查询

设置时间范围、阻断动作、规则编号、模块名称、协议名称、源接口、目的接口、源 IP 及端口、目的 IP 及端口、源 IP 及端口（NAT 后）、目的 IP 及端口（NAT 后）或描述信息的任意关键字，即可查询到相应的内容。

◆ 导出日志

在防火墙日志上方，单击导出图标即可将当前防火墙日志按照相应的格式保存到本地。

◆ 打印日志

在防火墙日志上方，单击图标即可将当前防火墙日志打印出来。打印报表之前，请确认打印机已正常连接。

7.2 入侵防护日志

通过查看入侵防护日志，可以方便管理员对入侵防护事件进行分析，如图 7.2 所示。

条件

时间范围 2009-08-12 10:00:00 - 2009-08-12 11:00:00

技术手段 全部

危险程度 全部

动作 全部

事件名称

协议摘要

接口

源地址

源MAC

源端口

目的地址

目的MAC

目的端口

查询 使用较短的词语查询时，可能得到预期外的结果

- 第1页 - [共 1 页] 转到第 页

	事件	源IP	源端口	目的IP	目的端口
08-12 16:55:02	[50083]Windows系统远程管理工具终端服务用户登录	10.10.20.251	4083	10.10.14.160	3389

eth7

C: 00:D0:C9:AC:BA:85

目的MAC: 00:06:5B:9F:94:E6

持续次数: 1

当前日志的导出（HTML、WORD、EXCEL 格式）和打印

图 7.2 日志分析 – 入侵防护日志

◆ **日志查询**

设置时间范围、技术手段、危险程度、阻断动作、事件名称、协议摘要、接口、源 IP/MAC 及端口或目的 IP/MAC 及端口的任意关键字，即可查询到相应的内容。

◆ **导出日志**

在入侵防护日志上方，单击导出图标即可将当前入侵防护日志按照相应的格式保存到本地。

◆ **打印日志**

在入侵防护日志上方，单击图标即可将当前入侵防护日志打印出来。打印之前，请确认打印机已正常连接。

7.3 IM/P2P 日志

通过查看 IM/P2P 日志，可以方便管理员对 IM/P2P 事件进行分析，如图 7.3 所示。

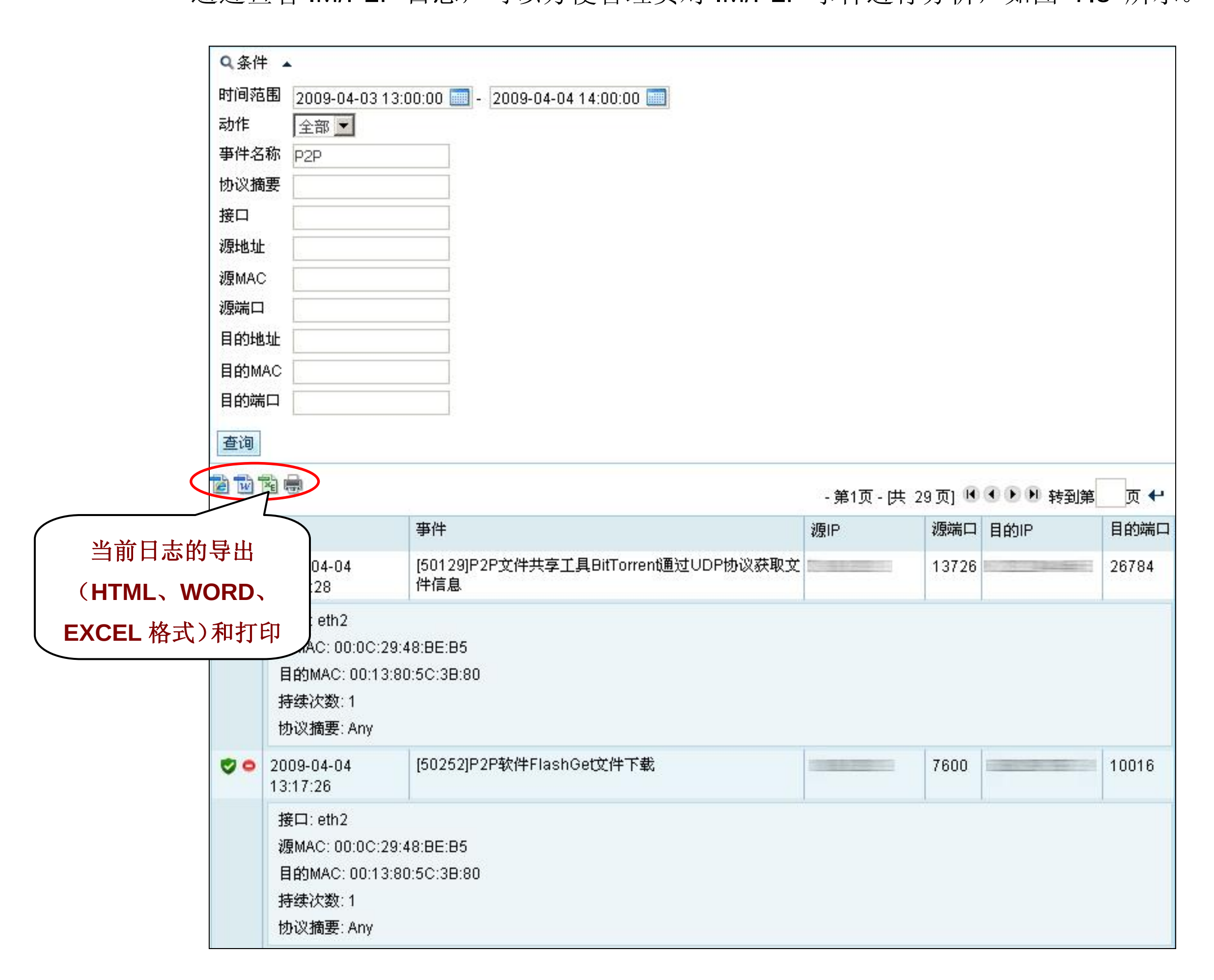


图 7.3 日志分析 – IM/P2P 日志

◆ **日志查询**

设置时间范围、阻断动作、事件名称、协议摘要、接口、源 IP/MAC 及端口或目的 IP/MAC 及端口的任意关键字，即可查询到相应的内容。

◆ **导出日志**

在 IM/P2P 日志上方，单击导出图标即可将当前 IM/P2P 日志按照相应的格式保存到本地。

◆ **打印日志**

在 IM/P2P 日志上方，单击图标即可将当前 IM/P2P 日志打印出来。打印之前，请确认打印机已正常连接。

7.4 WEB 安全日志

通过查看 WEB 安全日志，可以方便管理员对 WEB 安全事件进行分析，如图 7.4 所示。



图 7.4 日志分析 – WEB 安全日志

◆ 日志查询

设置时间范围、阻断动作、事件分类、站点、接口、源 IP/MAC 及端口或目的 IP/MAC 及端口的任意关键字，即可查询到相应的内容。

◆ 导出日志

在 WEB 安全日志上方，单击导出图标即可将当前 WEB 安全日志按照相应的格式保存到本地。

◆ 打印日志

在 WEB 安全日志上方，单击图标即可将当前 WEB 安全日志打印出来。打印之前，请确认打印机已正常连接。

7.5 防病毒日志

通过查看防病毒日志，方便管理员对网络数据中传输的病毒信息进行检查，包括病毒来源地址、目的地址和协议摘要等，如图 7.5 所示。



图 7.5 日志分析 – 防病毒日志

◆ 日志查询

设置时间范围、阻断动作、事件名称、协议摘要、接口、源 IP/MAC 及端口或目的 IP/MAC 及端口的任意关键字，即可查询到相应的内容。

◆ 导出日志

在防病毒日志上方，单击导出图标即可将当前防病毒日志按照相应的格式保存到本地。

◆ 打印日志

在防病毒日志上方，单击图标即可将当前防病毒日志打印出来。打印之前，请确认打印机已正常连接。

7.6 系统日志

系统日志包括所有登录日志、操作日志和系统启动日志，如图 7.6 所示。



图 7.6 日志分析 – 系统日志

◆ 日志查询

设置时间范围、用户名、登录 IP 或事件名称的任意关键字，即可查询到相应的内容。

◆ 导出日志

在系统日志上方，单击导出图标即可将当前系统日志按照相应的格式保存到本地。

◆ 打印日志

在系统日志上方，单击图标即可将当前系统日志打印出来。打印之前，请确认打印机已正常连接。

八. 统计报表

用户在此可以查看 NSFOCUS NIPS 的各类统计报表，包括防火墙报表、入侵防护报表、IM/P2P 报表、WEB 安全报表和防病毒报表，还可以将报表导出或打印，以便于统计分析。

8.1 防火墙统计报表

在防火墙统计报表中，根据指定的查询条件，可以查看符合条件的防火墙事件的统计图表，包括全部事件的源/目的地址 TOP10 和阻断事件的源/目的地址 TOP10，如图 8.1 所示。

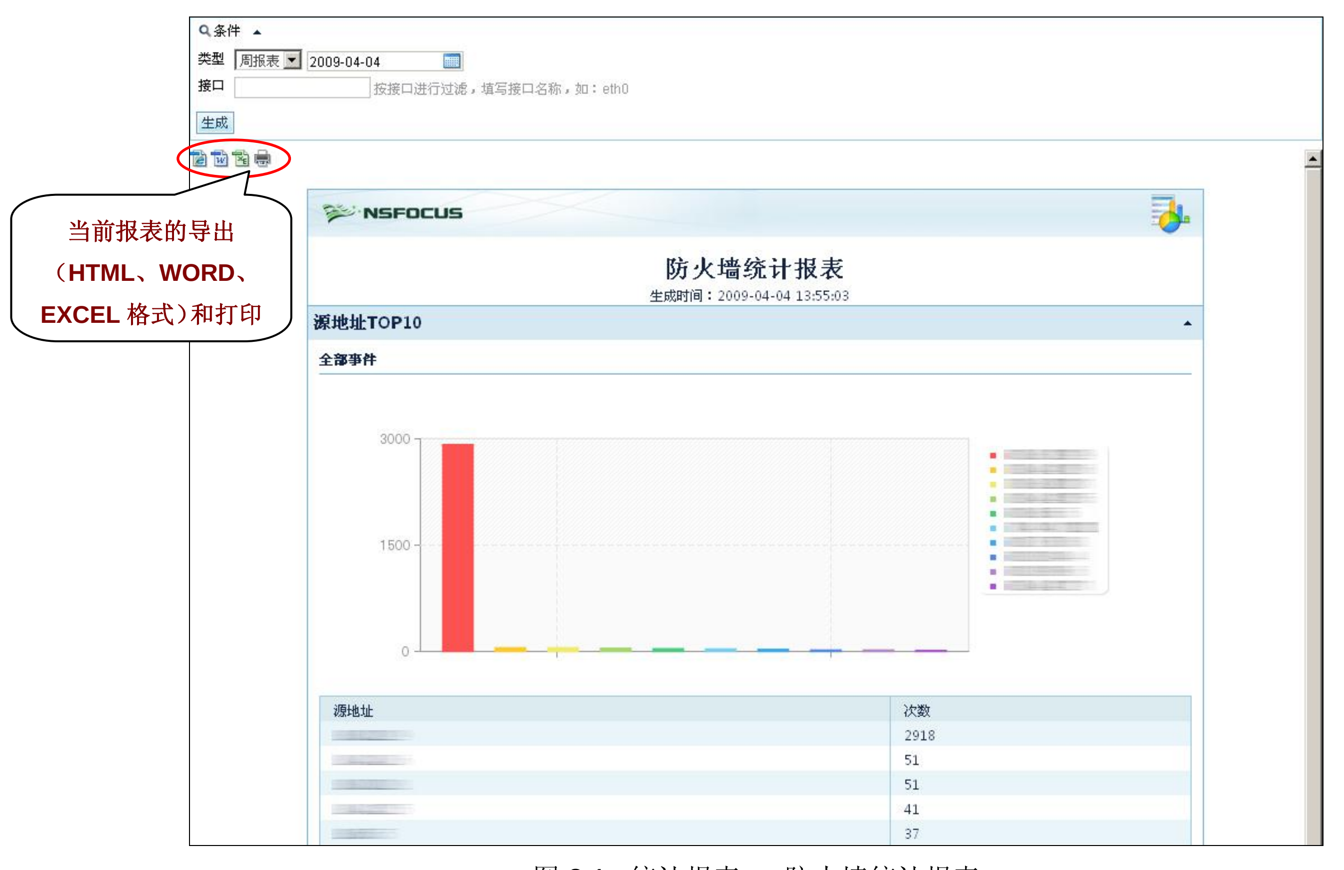


图 8.1 统计报表 – 防火墙统计报表

8.2 入侵防护统计报表

在入侵防护统计报表中，根据指定的查询条件，可以查看符合条件的入侵防护事件的统计图表，包括全部事件的源/目的地址 TOP10、阻断事件的源/目的地址 TOP10、全部事件 TOP10 和阻断事件 TOP10，如图 8.2 所示。

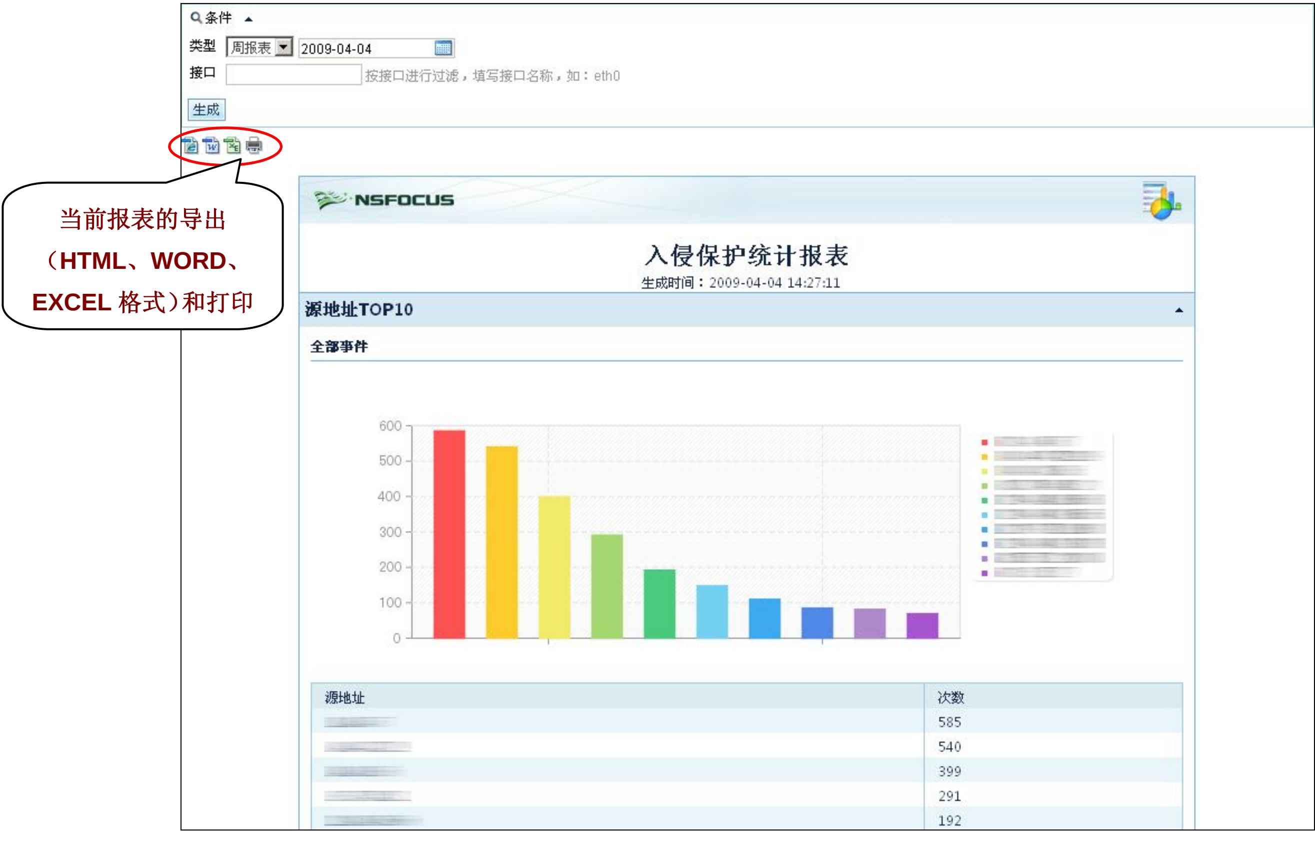


图 8.2 统计报表 – 入侵防护统计报表

8.3 IM/P2P 统计报表

在 IM/P2P 统计报表中，根据指定的查询条件，可以查看符合条件的 IM/P2P 事件的统计图表，包括全部事件的源/目的地址 TOP10、阻断事件的源/目的地址 TOP10、全部事件 TOP10 和阻断事件 TOP10，如图 8.3 所示。

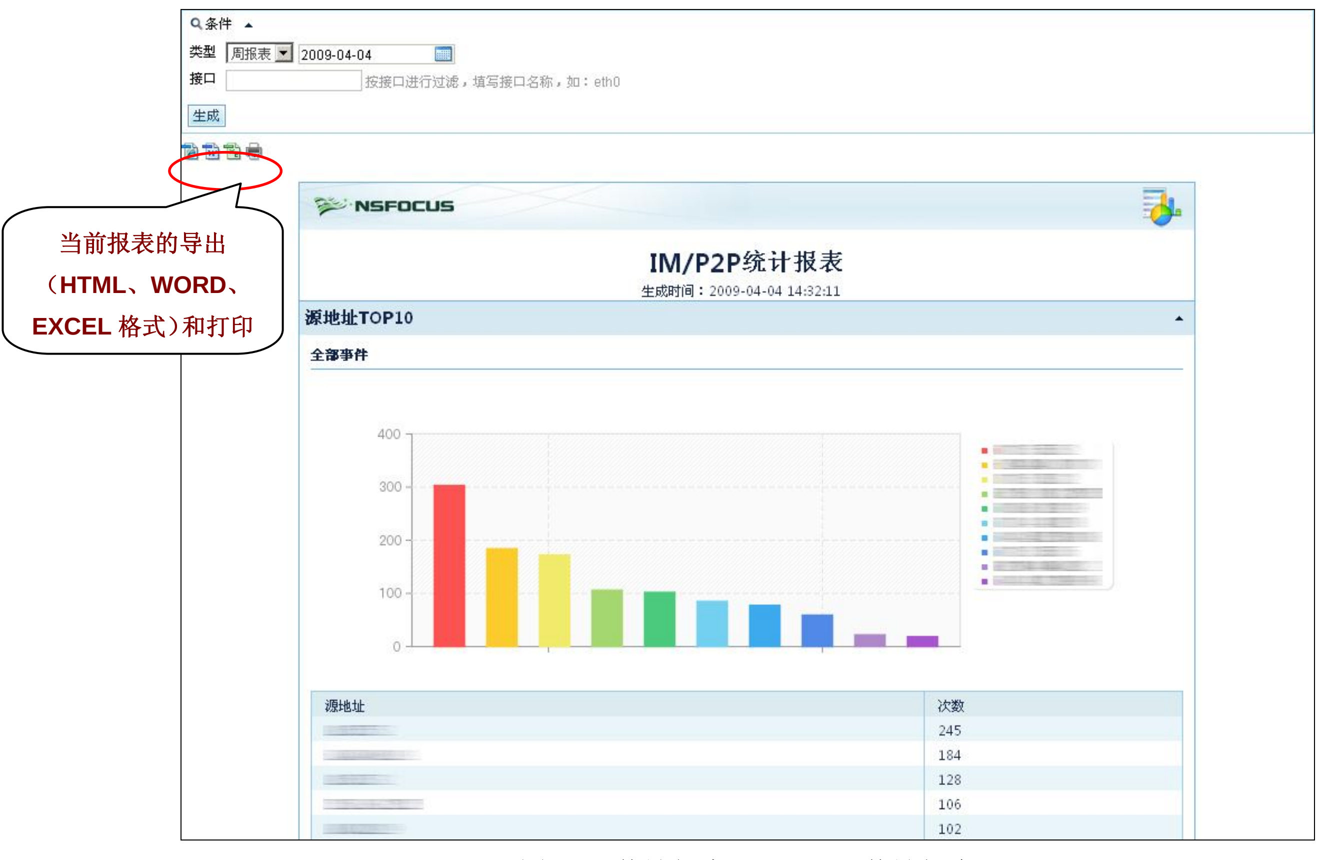


图 8.3 统计报表 – IM/P2P 统计报表

8.4 WEB 安全统计报表

在 WEB 安全统计报表中，根据指定的查询条件，可以查看符合条件的 WEB 安全事件的统计图表，包括全部事件的源/目的地址 TOP10、阻断事件的源/目的地址 TOP10、全部分类访问事件 TOP10、全部站点访问事件 TOP10、分类访问阻断事件 TOP10 和站点访问阻断事件 TOP10，如图 8.4 所示。

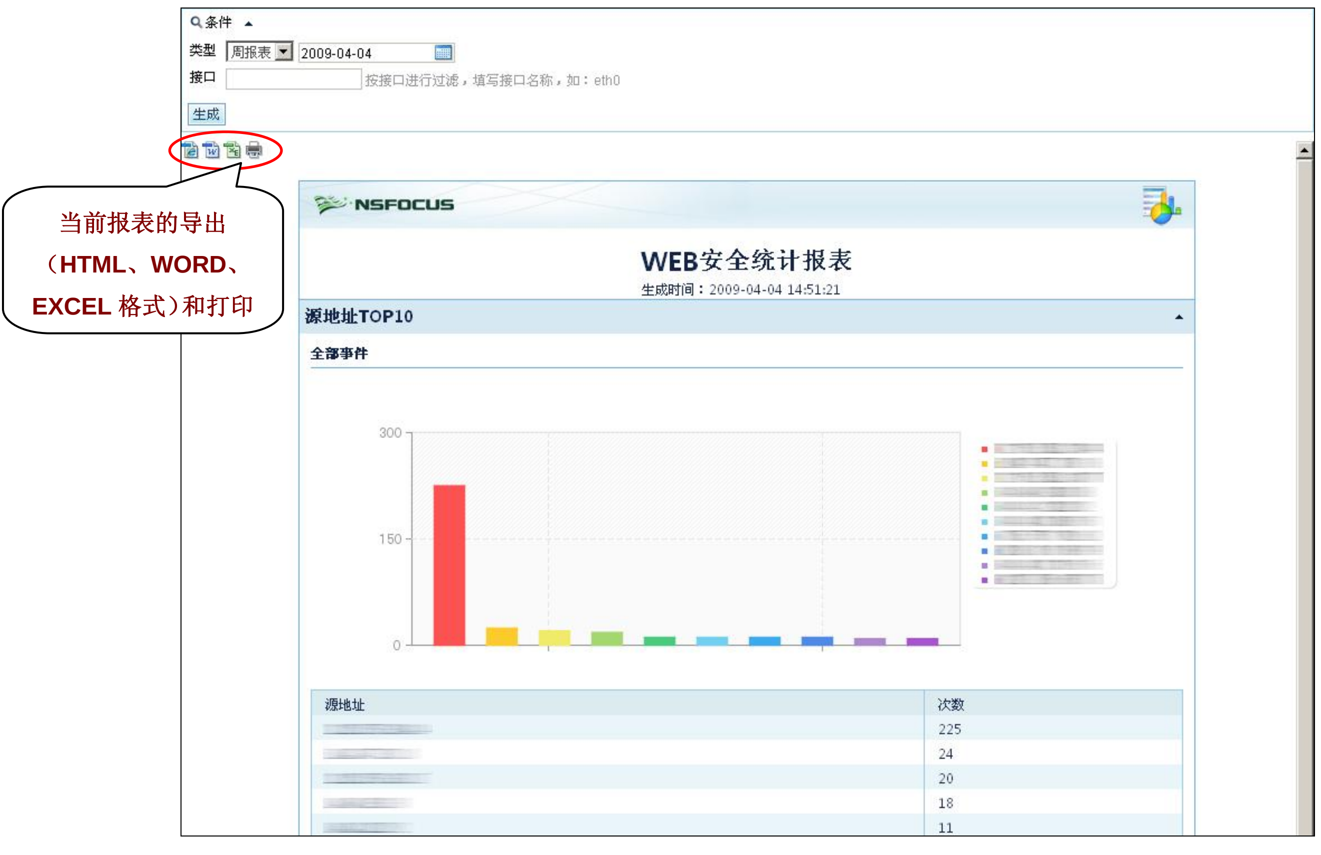


图 8.4 统计报表 – WEB 安全统计报表

8.5 防病毒统计报表

在防病毒统计报表中，根据指定的查询条件，可以查看符合条件的防病毒事件的统计图表，包括全部事件的源/目的地址 TOP10 和阻断事件的源/目的地址 TOP10，如图 8.5 所示。



图 8.5 统计报表 – 防病毒统计报表

九. 系统维护

9.1 升级与恢复

选择菜单【系统】➔【升级恢复】，进入设置升级方式和导入升级文件的页面。

9.1.1 升级设置

系统升级的方式有以下两种：

◆ 自动升级

系统默认启用自动升级，即可每日自动检测新的升级包，当检测到新升级包后会在凌晨自动升级所有规则文件，包括系统规则库文件、IM/P2P 规则库文件、病毒库文件、垃圾邮件库文件和 WEB 信誉库文件，无需管理员手动干预。

◆ 手动升级

由于自动升级发生在凌晨，当需要即时升级规则文件时可采用手动升级的方式。单击【手动升级】即可连接到绿盟科技的官方网站进行升级。

无论自动升级还是手动升级，前提条件是 NSFOCUS NIPS 可访问互联网。管理员需要在 DNS 客户端中配置适当的 DNS 服务器地址，以便能连接到绿盟科技的官方网站进行升级，具体配置请参见 5.12.2 DNS 客户端配置。同时注意接口配置中不要包含 DNS 服务器地址，否则会有地址冲突导致升级不成功。

在自动升级/手动升级时，只会升级规则文件，而引擎升级包需要管理员手工导入进行升级。

9.1.2 导入升级文件

升级文件的导入页面如图 9.1 所示。

导入系统升级文件	浏览... 上传 说明：导入系统升级文件（*.bin），引擎可能会自动重启
恢复全部配置备份文件	浏览... 上传 说明：恢复全部配置备份文件（*.ebk），恢复后要求重启系统才能生效
导入引擎参数文件	浏览... 上传 说明：导入引擎参数文件（*.xml），引擎会自动重启
导入流媒体服务器列表文件	浏览... 上传 说明：导入流媒体服务器文件（*.conf），引擎会自动重启 每行的格式为IP:掩码或IP:支持网段（例如1.1.1.1:255.255.255.0或1.1.1.1:24），能极大的降低流媒体应用如视频、语音的延时
导入本地认证文件	浏览... 上传 说明：导入本地认证文件（*.list），文件只能为ANSI编码，并且用户名和密码只能使用英文字母或数字。 格式为一行一个用户名和密码，用户名在前，密码在后，中间用逗号（,）隔开（如：admin,nsfocus）
导入用户自定义规则库文件	浏览... 上传 说明：导入用户自定义规则库文件（*.xml），自动加载生效
导入系统规则库文件	浏览... 上传 说明：导入系统规则库文件（*.xml），自动加载生效
导入病毒库升级文件	浏览... 上传 说明：导入病毒库升级文件（*.av），引擎可能会自动重启
导入垃圾邮件库升级文件	浏览... 上传 说明：导入邮件库升级文件（*.as），引擎可能会自动重启
导入恶意站点库文件	浏览... 上传 说明：导入恶意站点库文件（*.wcs），引擎可能会自动重启
导入URL分类库	浏览... 上传 说明：导入URL分类库文件（*.urlib），自动加载生效

图 9.1　系统 – 导入升级文件

请在此导入以下文件：

系统升级文件——NSFOCUS NIPS 的系统升级文件（*.bin），导入后引擎可能会自动重启。

引擎参数文件——NSFOCUS NIPS 的引擎参数文件（*.xml），导入后引擎会自动重启。

流媒体服务器列表文件——NSFOCUS NIPS 流媒体服务器文件（*.conf），导入后引擎会自动重启。

本地认证文件——NSFOCUS NIPS 的本地认证文件（*.list），导入后引擎可能会自动重启。

用户自定义规则库文件——NSFOCUS NIPS 自定义规则库模板文件（*.xml），导入后引擎会自动加载生效。

系统规则库文件——NSFOCUS NIPS 系统规则库模板文件（*.xml），导入后引擎会自动加载生效。

病毒库升级文件——NSFOCUS NIPS 病毒库升级文件（*.av），导入后引擎可能会自动重启。

垃圾邮件库升级文件——NSFOCUS NIPS 垃圾邮件库升级文件（*.as），导入后引擎可能会自动重启。

恶意站点库文件——NSFOCUS NIPS 恶意站点库文件（*.wcs），导入后引擎可能会自动重启。

URL 分类库文件——NSFOCUS NIPS URL 分类库文件（*.urlib），导入后引擎会自动加载生效。

除了可以导入上述各类文件外，还可以恢复全部配置文件（*.ebk），恢复后要求重启系统才能生效。

9.2 下载与备份

选择菜单【系统】➔【下载备份】，进入下载文件的页面，如图 9.2 所示。请按照说明下载相应的文件。



图 9.2 系统 – 下载文件

9.3 系统配置

9.3.1 引擎配置

如图 9.3 所示，进行 NSFOCUS NIPS 引擎的配置管理，各项参数配置完毕，单击【确定】。

远程协助	⊙开启 ○关闭
Ping(Icmp)	⊙开启 ○关闭
SnmpTrap	⊙开启 ○关闭
SnmpTrap主机	10.10.11.220
SnmpAgent	○开启 ⊙关闭
时间同步	○开启 ⊙关闭
设备名称	
设备位置	
强制硬件bypass	○开启 ⊙关闭
	确定

图 9.3 系统 – 引擎配置

引擎的主要参数含义如下：

远程协助——选择**开启**，可以通过 50022 端口进行远程管理（仅限绿盟科技的技术人员在网络调试时使用）。

Ping(Icmp)——选择**开启**，允许当前 NSFOCUS NIPS 设备对 Icmp 请求作出应答，方便管理员调试设备故障；选择**关闭**，表示当前 NSFOCUS NIPS 设备对 Icmp 请求不作出应答。

SnmpTrap 主机——指定接收 NSFOCUS NIPS 告警事件 trap 信息的服务器 IP 地址。若不指定，请置为**关闭**。

SnmpAgent——选择**开启**，表示开启 Snmp 代理功能。

时间同步——选择**开启**，指定时间同步服务器的 IP 地址（保证引擎管理口和该时间同步服务器能够正常通讯），将 NSFOCUS NIPS 的系统时间与其同步（时间同步间隔的单位：秒）。若不指定，请置为**关闭**。开启时间同步功能后，需要重启系统才能生效。

强制硬件 bypass——选择**开启**，表示设备将被强制进入 bypass 状态。

9.3.2 外置 Bypass 配置

当 NSFOCUS NIPS 开启与外置 Bypass 交换机的联动时，需要选择菜单【网络】➔【外置 Bypass】，根据实际情况设置 Bypass 设备 1~4 的 IP 地址和访问密码以及外置 Bypass 交换机的心跳信号控制口和接口地址，如图 9.4 所示。

工作状态 ⦿开启 ○关闭

设备1		设备2	
地址	0.0.0.0	地址	0.0.0.0
密码	••••	密码	••••
心跳口		心跳口	
接口对		接口对	

设备3		设备4	
地址	0.0.0.0	地址	0.0.0.0
密码	••••	密码	••••
心跳口		心跳口	
接口对		接口对	

确定

图 9.4 系统 – 外置 Bypass 设备

开启外置 Bypass 开关后，需要保证 NSFOCUS NIPS 设备自身的带外管理口与外置 Bypass 交换机之间能够通信。有关外置 Bypass 交换机的安装及使用方法，请查阅相应设备随机附带的用户使用说明书。

9.3.3 与安全中心连接

选择菜单【系统】➔【系统配置】➔【安全中心】，进入 NSFOCUS NIPS 引擎与绿盟安全中心连接的配置页面，如图 9.5 所示。在这里可以配置引擎的本机数据传输地址、主安全中心 IP 地址和所要连接的安全中心 IP 地址。



图 9.5 系统 – 配置引擎的安全中心

下面介绍部分参数的含义：

本机数据传输地址——指定引擎用于和绿盟安全中心通讯的 IP 地址，通常为某个接口的管理 IP。

引擎的主安全中心 IP 地址——指定主安全中心的 IP 地址，它可以对引擎有一定控制权，包括远程启动/停止、升级、获得归并日志等控制管理权限。

引擎的 x 号安全中心 IP 地址——指定需要引擎进行主动连接的安全中心的 IP 地址，对于由绿盟安全中心向引擎主动连接的安全中心，则不需要在此设置，在使用中请检查引擎和绿盟安全中心两端的配置以避免冲突。

配置以上各参数信息时，需注意以下三点：

- “引擎的主安全中心 IP 地址”仅仅是设置主安全中心的 IP，在安全中心添加了需要管理的引擎后，还需同时在 x 号安全中心 IP 地址中填上所要连接的安全中心的 IP 地址。
- 设置“引擎的 x 号安全中心 IP 地址”时，最多可设置 4 个从引擎主动发起连接的绿盟安全中心。
- 若要在安全中心接收防火墙日志，必须修改 config.xml 中的参数，如下所示（安全中心的 IP 地址是 192.168.100.100）。

```
syslog host="192.168.100.100"
```

9.3.4 SQL 注入白名单

当入侵防护规则的事件对象中包含**[29001]WEB 服务远程 SQL 注入攻击**规则时，若是希望该规则对某些服务器不起防护作用，即可设置 SQL 注入白名单，将这些服务器的 URL 添加进来。

选择菜单【系统】➔【系统配置】➔【SQL 注入白名单】，进入 SQL 注入白名单配置界面，添加不需要防护服务器的 URL，如图 9.6 所示。



图 9.6 系统配置 –SQL 注入白名单

填写 SQL 注入白名单的格式如下：

a. 填写主机名及其域名，用“/”隔开；

b. 每行填写一个主机，例如 www.google.cn/zh-CN。

9.3.5 恶意站点库白名单

当用户确认一个站点或服务器是可信的，没有恶意代码时，即可设置恶意站点库白名单。选择菜单【系统】➔【系统配置】➔【恶意站点库白名单】，进入恶意站点库白名单配置界面，将确认可信的站点或服务器的 URL 添加进来，如图 9.7 所示。

⚠每行只能填写一个 URL 地址。



图 9.7　系统配置 –恶意站点库白名单

9.4 帐号管理

在帐号管理界面下，可以管理登录设备的帐号，并对登录过程中的参数进行配置。.

9.4.1 帐号管理

系统有两个默认的账户：缺省操作员 weboper 和缺省审计员 webaudit，它们各自的功能如下：

weboper：负责除系统日志查看外的配置和管理。

webaudit：负责系统日志的查看和审计员账号的管理。

当用户以缺省操作员 weboper 帐号登录设备时，选择菜单【系统】➔【帐号管理】，即可进入设置帐号的页面，如图 9.8 所示。

帐号管理 参数配置

新建

用户帐号	角色	允许登录IP	邮箱	启用	配置
weboper	操作员	*	weboper@nsfocus.com		

图 9.8 系统 – 帐号管理

以系统缺省的操作员 weboper 帐号登录设备时，帐号列表中只显示操作员用户信息。在此可以进行操作员帐号的添加、修改和删除等操作。

以系统缺省的审计员 webaudit 帐号登录时，帐号列表中只显示审计员用户信息。在此可以进行审计员帐号的添加、修改和删除等操作。

⚠缺省的帐号 weboper 和 webaudit 帐号都不允许被修改和删除。

下表列出不同角色的账号分别具有哪些操作权限。

用户组	权限
缺省的操作员 weboper	除查看日志分析->系统日志外的所有操作权限
新建的读写操作员	除查看日志分析->系统日志和账号管理->账号管理外的所有操作权限
新建的读操作员	除查看日志分析->系统日志和账号管理->账号管理外的所有读操作权限
缺省的审计员 webaudit	有登录退出、修改当前用户密码、审计员帐号管理、切换语言、查看系统日志的权限。
新建的审计员	有登录退出、修改当前用户密码、切换语言、查看系统日志的权限。

⚠**只有缺省操作员和缺省审计员才有权限对相应帐号管理，做添加、修改和删除操作。**

新建的操作员和审计员无帐号管理权限，只有修改当前用户密码的权限。

◆ **添加帐号**

以缺省操作员登录设备，在图 9.8 所示的界面中，单击图形右方的【新建】按钮，弹出如图 9.9 所示的界面。在该界面下输入帐号信息，单击【确认】，添加帐号。

新建
密码
密码确认
允许登录IP *
电子邮箱
角色 操作员(读写) 操作员(读)
确 定 取 消

图 9.9 添加新账户

添加帐号时，需填写以下信息：

用户帐号——即登录 ID，长度必须在 6 至 20 个字符之间，可以由数字、字母或下划线组成，用户名开头不能是数字。

密码——即登录密码，不能和用户名相同，长度必须在 6 至 20 个字符之间，不能包含空格，且不能全为数字或全为字母。

电子邮箱——该用户有效的电子邮件地址（此项不是必填项）。

角色——每个帐号角色拥有的权限不同，请选择该帐号隶属于哪个角色。

◆ **修改帐号**

以缺省操作员登录设备，在图 9.8 所示的界面中，单击配置下方的图标，可以修改对应的帐号信息。

修改帐号信息时，除了用户帐号以外，其余各项均可修改。

修改系统缺省帐号 webaudit 和 weboper 的信息时，只能修改其登录密码和电子邮箱。

◆ **删除帐号**

缺省操作员和缺省审计员可以删除各自新建的账户，但不允许删除系统缺省帐号 webaudit 和 weboper。

如果修改过系统缺省帐号的密码且不小心遗忘，可以通过引擎串口管理界面重置密码，详细操作方法请参见 10.3.4 维护工具。

9.4.2 参数配置

选择菜单【系统】➔【帐号管理】➔【参数配置】，进入参数配置页面，如图 9.10 所示。在该界面下，通过输入不同的参数，可以对登录过程进行管理。

帐号管理 参数配置

登录尝试次数	3
登录间隔时间（分钟）	3
登录多次失败后的处理方式	☐ 封用户 说明：封IP功能默认开启
最小密码长度	8

确定

图 9.10 帐号管理－参数配置

详细参数说明如下：

登录尝试次数——用户在设定的登陆时间间隔内，连续错误登陆的次数。默认为 3 次。

登录间隔时间——用户在规定的登录尝试次数内没有成功登录设备后，可以重新登录设备的时间间隔。默认为 3 分钟。

用户登录失败后 IP 地址被系统默认封锁，直到超过设定的登录间隔时间解锁，才可以重新登录设备。

登录多次失败后的处理方式——封锁超过登录尝试次数的用户帐号。选择该功能后，即使用户改变 IP 地址重新登录，也能被系统封锁。

最小密码长度——可以设定用户帐号的密码最小长度，默认为 8 位。

9.5 网络诊断与调试

选择菜单【系统】➔【诊断工具】，即可在此查看当前网络的连接状态和网卡状态，如果发生异常情况，可通过 ping 或 traceroute 等工具进行相应的诊断和查看。

9.5.1 网络连接状态

如图 9.11 所示，显示当前网络的连接状态。

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 0.0.0.0:50001 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:50002 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:50004 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:50002 127.0.0.1:35698 ESTABLISHED
tcp 0 0 127.0.0.1:35698 127.0.0.1:50002 ESTABLISHED
tcp 0 0 :::50022 :::* LISTEN
tcp 0 0 :::442 :::* LISTEN
tcp 0 0 :::443 :::* LISTEN
tcp 0 0 ::ffff:10.8.8.10:443 ::ffff:192.168.5.2:1240 ESTABLISHED
tcp 0 0 ::ffff:10.8.8.10:443 ::ffff:192.168.5.2:1229 TIME_WAIT
tcp 0 0 ::ffff:10.8.8.10:443 ::ffff:192.168.5.2:1237 TIME_WAIT
tcp 0 0 ::ffff:10.8.8.10:443 ::ffff:192.168.5.2:1220 TIME_WAIT
tcp 0 0 ::ffff:10.8.8.10:443 ::ffff:192.168.5.2:1222 TIME_WAIT
tcp 0 0 ::ffff:10.8.8.10:443 ::ffff:192.168.5.2:1231 TIME_WAIT
tcp 0 0 ::ffff:10.8.8.10:443 ::ffff:192.168.5.2:1235 TIME_WAIT
tcp 0 0 ::ffff:10.8.8.10:443 ::ffff:192.168.5.2:1233 TIME_WAIT
tcp 0 0 ::ffff:10.8.8.10:443 ::ffff:192.168.5.2:1232 TIME_WAIT
tcp 0 0 ::ffff:10.8.8.10:443 ::ffff:192.168.5.2:1238 TIME_WAIT
tcp 0 0 ::ffff:10.8.8.10:443 ::ffff:192.168.5.2:1224 TIME_WAIT
tcp 0 0 ::ffff:10.8.8.10:443 ::ffff:192.168.5.2:1236 TIME_WAIT
tcp 0 0 ::ffff:10.8.8.10:50022 ::ffff:10.8.8.8:2889 ESTABLISHED
tcp 0 0 ::ffff:10.8.8.10:443 ::ffff:192.168.5.2:1223 TIME_WAIT
udp 0 0 0.0.0.0:32772 0.0.0.0:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags Type State I-Node Path
unix 2 [ ACC ] STREAM LISTENING 92 /var/run/acpid.socket
```

图 9.11　系统 – 当前的网络连接状态

9.5.2 网卡状态

如图 9.12 所示，显示当前的网卡状态。

```
eth0 Link encap:Ethernet HWaddr 00:90:FB:14:B0:8C
inet addr:10.8.8.10 Bcast:10.8.255.255 Mask:255.255.0.0

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:526619 errors:0 dropped:0 overruns:0 frame:0
TX packets:348993 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:68595374 (65.4 Mb) TX bytes:96215515 (91.7 Mb)

eth1 Link encap:Ethernet HWaddr 00:90:FB:14:B0:8D
inet addr:192.168.2.1 Bcast:192.168.2.255 Mask:255.255.255.0
inet6 addr: fe80::290:fbff:fe14:b08d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:43079233 errors:0 dropped:5 overruns:0 frame:0
TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:1677081456 (1599.3 Mb) TX bytes:468 (468.0 b)

eth2 Link encap:Ethernet HWaddr 00:90:FB:10:E3:44
inet addr:192.168.3.1 Bcast:192.168.3.255 Mask:255.255.255.0
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

图 9.12　系统 – 当前的网卡状态

9.5.3 ping 工具

ping 工具用于检测主机存活或网络通断情况。

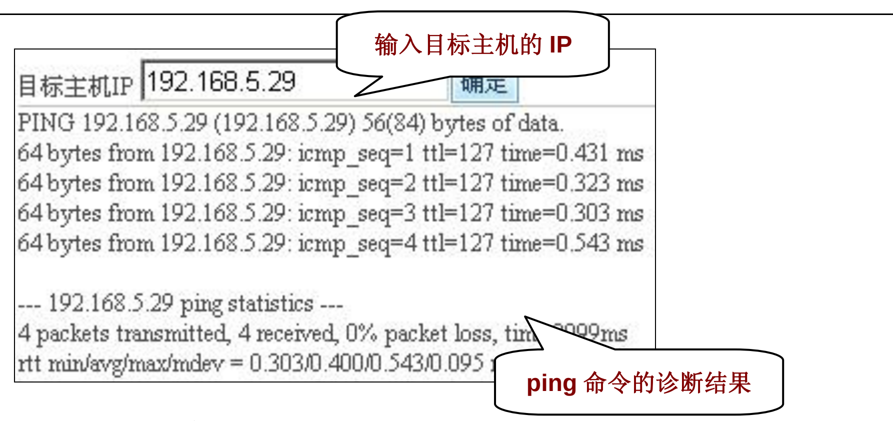


图 9.13 系统 – 网络诊断工具（ping 工具）

9.5.4 traceroute 工具

traceroute 即路由追踪，用于检测网络路由线路。

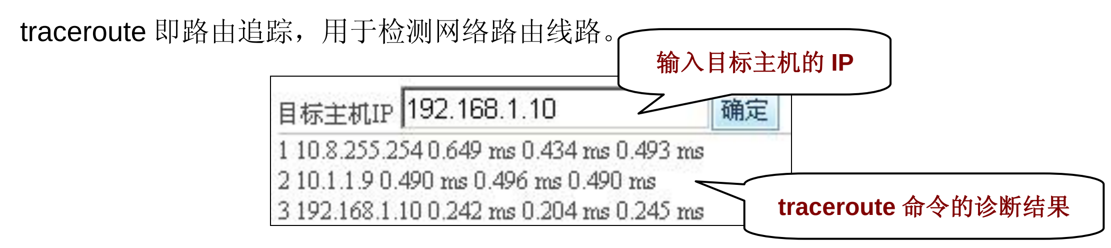


图 9.14 系统 – 网络诊断工具（traceroute 工具）

9.6 证书管理

选择菜单【系统】➔【证书管理】，用户可以在此进行证书更新管理。有关证书的导入方法，请参见 3.2 导入证书。

9.7 系统控制

选择菜单【系统】➔【系统控制】，进入系统控制的操作页面。如图 9.15 所示，通过单击相应的按钮可以进行以下系统控制的操作：

应用配置——除了接口以外，所有策略和引擎配置将被重新加载生效。这里的策略包括防火墙策略、入侵防护策略、流量管理策略、IM/P2P 策略、内容安全策略、WEB 安全策略、防病毒策略和反垃圾邮件策略。

重启引擎——重新启动引擎，所有策略和引擎配置将被重新加载生效，包括接口的配置。

重启系统——重新启动 NSFOCUS NIPS 硬件系统。

开始调试——进入网络调试的模式（仅限绿盟科技的技术人员在网络调试时使用）。

结束调试——退出网络调试的模式（仅限绿盟科技的技术人员在网络调试时使用）。

应用配置	策略将被重新加载生效。
重启引擎	重新启动引擎，策略和配置将被重新加载生效。
重启系统	重新启动整个硬件系统。
开始调试	进入调试模式。
结束调试	退出调试模式。

图 9.15　系统 – 系统控制

执行重启系统后，所有报表的数据将被清空，然后重新统计。

十. 引擎串口管理

10.1 功能概述

通过串口连接可以访问 NSFOCUS NIPS 引擎的串口管理界面，在此处提供给管理员一些系统初始配置、状态检测和恢复初始化配置等功能，Web 管理界面中无法进行管理的部分，可以在此进行管理操作。

10.2 登录串口

管理员登录引擎串口之前，需要做好以下准备工作：

- 工作计算机 1 台
- 随机附带的串口线 1 根
- 能够连接串口的终端软件（比如 Windows 自带的超级终端软件）
- 用串口线将 NSFOCUS NIPS 和工作计算机连接

下面以 Windows XP 自带的超级终端软件为例，详细介绍实际连接过程：

（1）选择菜单【开始】➔【程序】➔【附件】➔【通讯】➔【超级终端】，出现如图 10.1 所示窗口，单击【取消】，然后单击【是】并【确定】。

如果没有出现图 10.1 所示的窗口，可以跳过步骤（1）。



图 10.1 超级终端运行的位置信息

（2）在随即出现的连接描述窗口中，输入此次连接的名称（例如：*NIPS*），单击【确定】，如图 10.2 所示。



图 10.2 输入超级终端连接描述

（3）随后出现图 10.1 所示窗口，单击【取消】并确定。

（4）选择工作计算机连接串口线的串口设备（例如：选择 *COM1*），单击【确定】，如图 10.3 所示。



图 10.3 选择超级终端连接端口

（5）如图 10.4 所示，设置端口属性（每秒位数 115200，数据位 8）。



图 10.4 设置超级终端连接端口

（6）单击【确定】后按回车键，出现提示符 **login:** 这时输入串口管理员的用户名和密码（默认用户名和密码均是 conadmin）。

（7）如果用户名和密码正确无误，即可成功登录（连接后将终端类型设为 VT100，可以获得最佳显示效果）。

（8）成功登录网络引擎之后，出现引擎管理语言选择界面，如图 10.5 所示，选择 **1.中文**，按回车键，进入引擎管理中文菜单界面，如图 10.6 所示。



图 10.5 选择引擎管理菜单语言

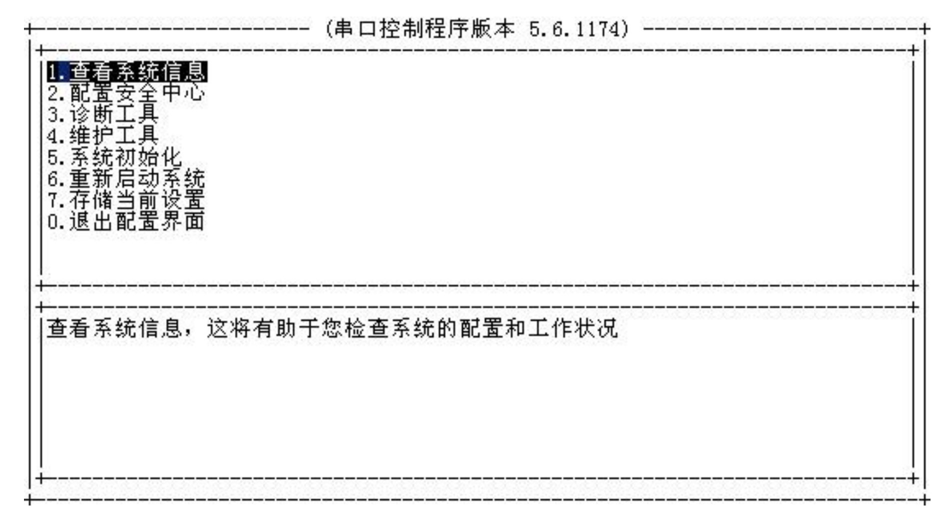


图 10.6　NSFOCUS NIPS 引擎的串口管理主菜单

在引擎管理界面中只能用键盘操作，下表对键盘各键含义进行说明。

键盘	含义
↑	①切换到输入框 ②上移
↓	①切换到【确定】 ②下移
←	①切换到【确定】 ②左移
→	①切换到【取消】 ②右移
Esc	直接取消
Enter	直接确认
Tab	在输入框、【确定】、【取消】之间切换
BackSpace	删除当前光标所在位置的前一字符

10.3 详细介绍

下面详细介绍 NSFOCUS NIPS 引擎的串口管理界面中各功能菜单的操作和含义。

10.3.1 查看系统信息

如图 10.7 所示，管理员可以进行以下操作：

显示接口设置——查看系统当前所有网络接口的信息，包括接口 IP、接口管理 IP 和所属安全区（引擎各网络接口的设置仅能在 Web 管理界面中修改，具体操作方法请参见 4.1.1 单路部署）。

显示远程安全中心配置——查看系统当前的远程安全中心配置（有关引擎远程安全中心参数的配置方法，请参见 10.3.2 配置安全中心）。

显示证书信息——查阅 NSFOCUS NIPS 的引擎证书，包括证书状态、证书类型、许可工作模式、支持硬件接口数量、颁发对象、颁发日期和截止日期等。

设置系统时钟——设置系统时钟，以供通讯和日志记录时使用。

设置系统时区——设置系统时区，方便引擎位于其他时区时的使用（默认为东 8 时区，取值范围为-12 到 12）。

硬件特征值——硬件特征值是每台网络引擎的唯一标识，在给其制作证书时需要获取该值。

产品状态值——该值是提供给绿盟科技工程人员使用的内部口令，每天会变化一次。

产品版本信息——显示当前引擎版本和引擎固件版本的详细信息。

返回上级菜单——返回到上一级配置菜单中。



图 10.7 引擎串口管理 – 查看系统信息

NSFOCUS NIPS 出厂时未配置证书，可以通过引擎的 Web 管理界面进行证书导入。有关导入引擎证书的操作方法，请参见 3.2 导入证书。

10.3.2 配置安全中心

如图 10.8 所示，配置 NSFOCUS NIPS 引擎与绿盟安全中心建立连接的各项参数：

设置本机数据传输地址——设置 NSFOCUS NIPS 引擎通信接口的网络 IP 地址，供其与绿盟安全中心进行网络通讯，以及 Web 管理模式。

设置主安全中心 IP 地址——指定主安全中心的 IP 地址，它可以对引擎有一定控制权，包括远程启动/停止、升级、获得归并日志等控制管理权限（在此仅仅是设置主安全中心的 IP，与主安全中心的连接参数还需要另外设置，比如设置 x 号安全中心 IP 地址）。

设置 x 号安全中心 IP 地址——指定需要引擎进行主动连接的绿盟安全中心的 IP 地址（最多可设置 4 个从引擎主动发起连接的绿盟安全中心）。

返回上级菜单——返回到上一级配置菜单中。

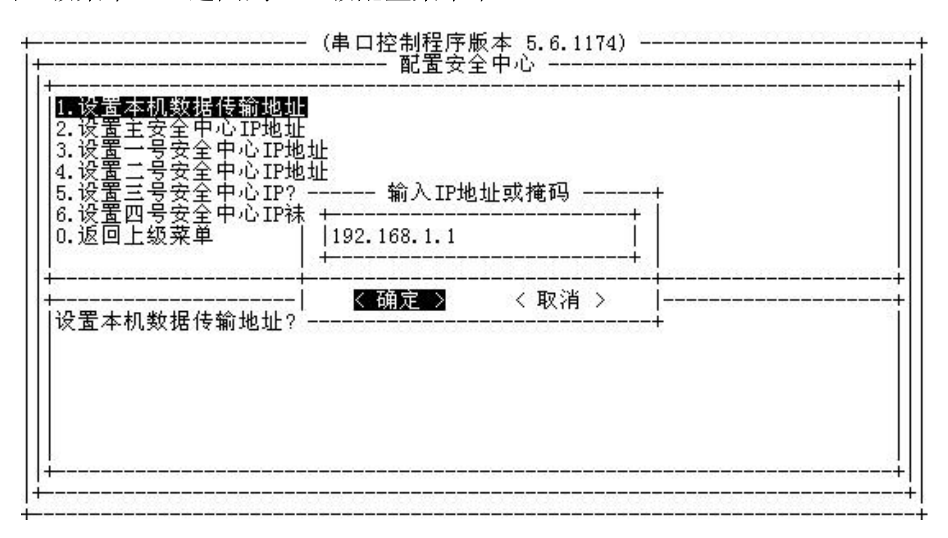


图 10.8　引擎串口管理 – 配置网络引擎参数

10.3.3 诊断工具

如图 10.9 所示，此处包括 UNIX 标准下的一些系统诊断工具，管理员可利用它们检查网络状况和排除系统安装中的困难。

Ping——检查引擎与目标 IP 地址的连接状况。

追踪路线——检查沿途路由设备的转发情况。

网络状态——检查引擎与绿盟安全中心的通讯连接情况。

显示路由信息——查看引擎上当前配置的路由表信息。

网卡信息——查看引擎的网卡信息。

返回上级菜单——返回到上一级配置菜单中。

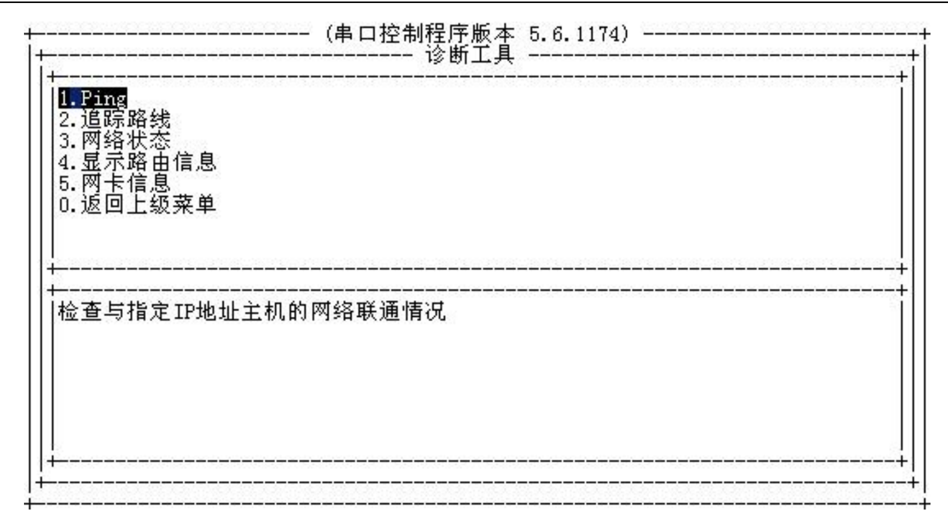


图 10.9 引擎串口管理 – 诊断工具

管理员也可以在 NSFOCUS NIPS 引擎的 Web 管理中使用诊断工具，相关操作方法请参见 9.5 网络诊断与调试。

10.3.4 维护工具

如图 10.10 所示，管理员可以进行以下操作：

设置管理员密码——设置引擎管理界面登录帐号 conadmin 的密码（请妥善保管此密码，如果忘记，将不能通过串口配置系统，必须联系绿盟科技的技术支持人员重置密码）。

设置 CLI 管理员密码——设置 CLI 管理界面登录帐号 shell 的密码（请妥善保管此密码，如果忘记，将不能通过 CLI 管理界面配置动态路由，必须联系绿盟科技的技术支持人员重置密码）。

重置 Web 用户——重置 Web 管理模式下的系统用户信息，其中，系统的两个缺省用户（weboper 和 webaudit）的密码等信息被重置；自定义的用户信息全部被删除。

清空临时文件——清除引擎在运行中产生的临时文件（一般情况下，不建议清空临时文件。执行此项操作后，若出现无法正常使用 Web 管理或其他问题，请重启 NSFOCUS NIPS 引擎系统，以保证正常使用）。

关闭远程协助——远程协助默认是关闭状态，在此按回车键后改为开启状态。

禁止 Ping（Icmp）——Ping（Icmp）默认是开启状态，在此按回车键后改为禁止状态。

关闭强制硬件 Bypass——仅用于关闭强制硬件 Bypass（重启系统后该设置生效），完成此操作之后必须存储当前设置。在此不提供开启强制硬件 Bypass 功能。

返回上级菜单——返回到上一级配置菜单中。

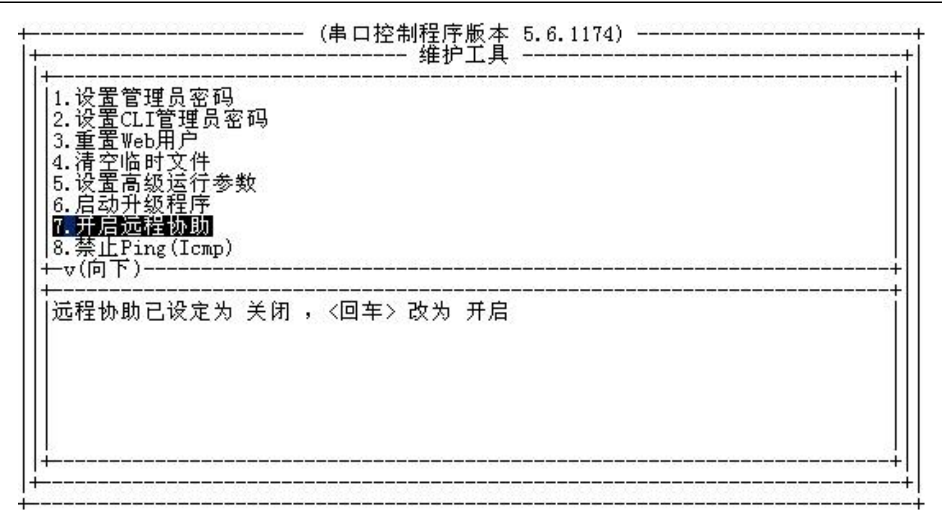


图 10.10　引擎串口管理 – 维护工具

10.3.5 系统初始化

如图 10.11 所示，初始化 NSFOCUS NIPS 的配置，系统会将程序文件或全部数据恢复到初始状态，包括密码和配置。

初始化配置——将所有配置初始化为出厂状态（其中，系统时钟和对象配置文件不会改变），但硬件证书会被删除，初始化配置之前，请确认证书的副本是否已经保存。

恢复系统——所有程序和设置都会被恢复为出厂状态，但硬件设备证书会自动保存。

返回上级菜单——返回到上一级配置菜单中。

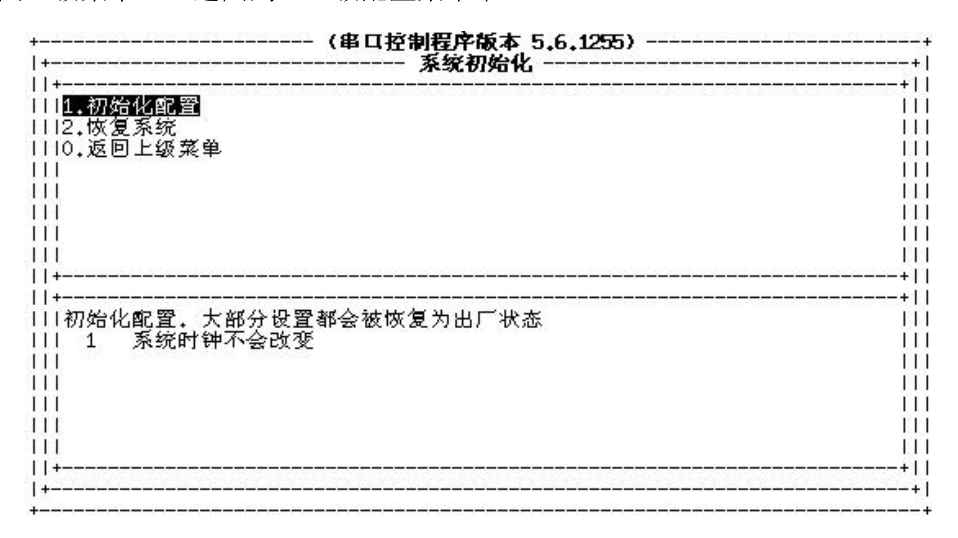


图 10.11　引擎串口管理 – 系统初始化

执行【初始化配置】后，需要重启系统才能生效。

10.3.6 重新启动系统

如图 10.12 所示，选择【是】即可重新启动 NSFOCUS NIPS 引擎；选择【否】，则返回到当前菜单。

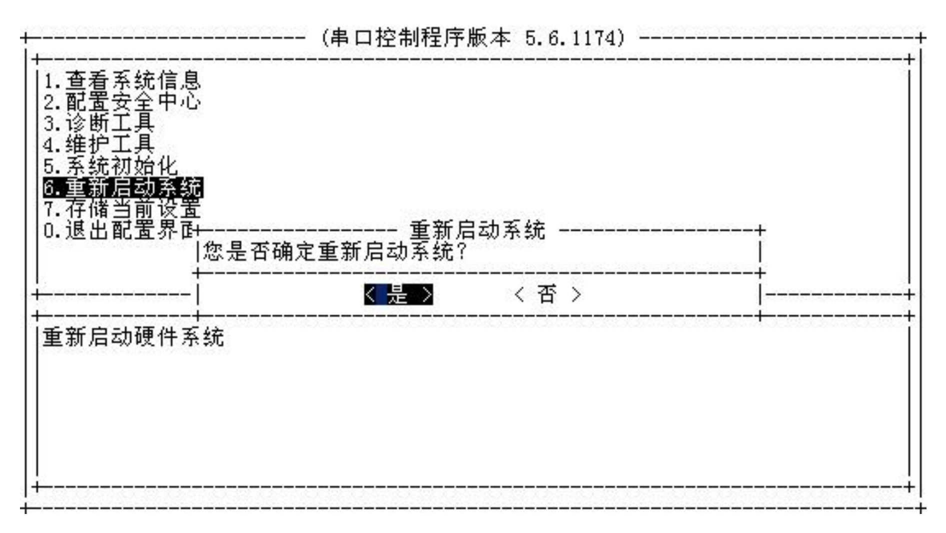


图 10.12 引擎串口管理 – 重新启动系统

10.3.7 存储当前设置

如图 10.13 所示，选择【是】即可将当前配置存入存储器并生效；选择【否】，则取消保存，并返回到当前菜单。

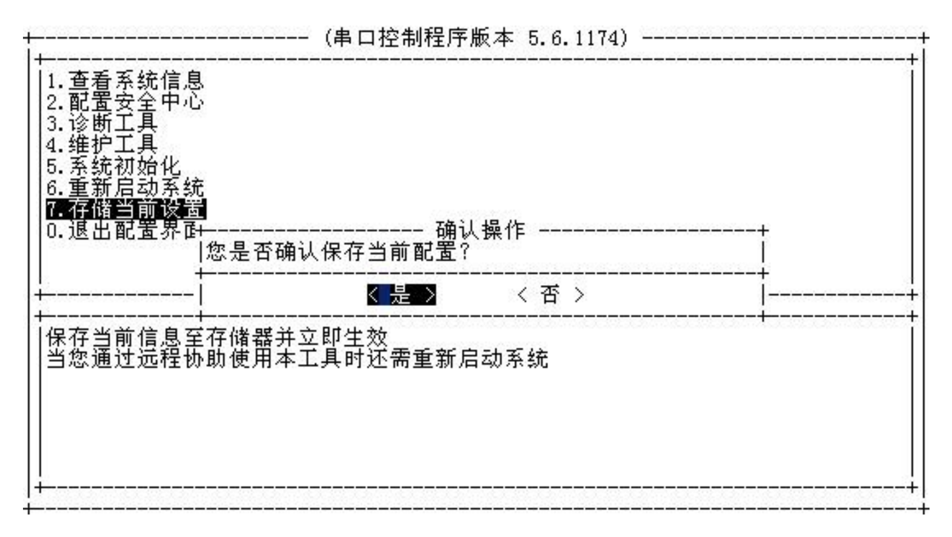


图 10.13 引擎串口管理 – 存储当前设置

10.3.8 退出配置界面

NSFOCUS NIPS 引擎各项配置完毕，将光标移到 **0.退出配置界面**，按回车键将退出 NSFOCUS NIPS 引擎串口配置界面。退出前系统将会提示是否保存当前配置，选择【是】则保存退出，选择【否】则不保存退出。退出后如需再次配置，请重新登录。

十一. NSFOCUS NIPS 规则库

选择菜单【帮助】➔【帮助】，可以查询 NSFOCUS NIPS 规则库中详细的规则信息，如图 11.1 所示。用户可以按照规则编号或规则描述进行搜索，也可以直接单击【查询】列出全部规则。

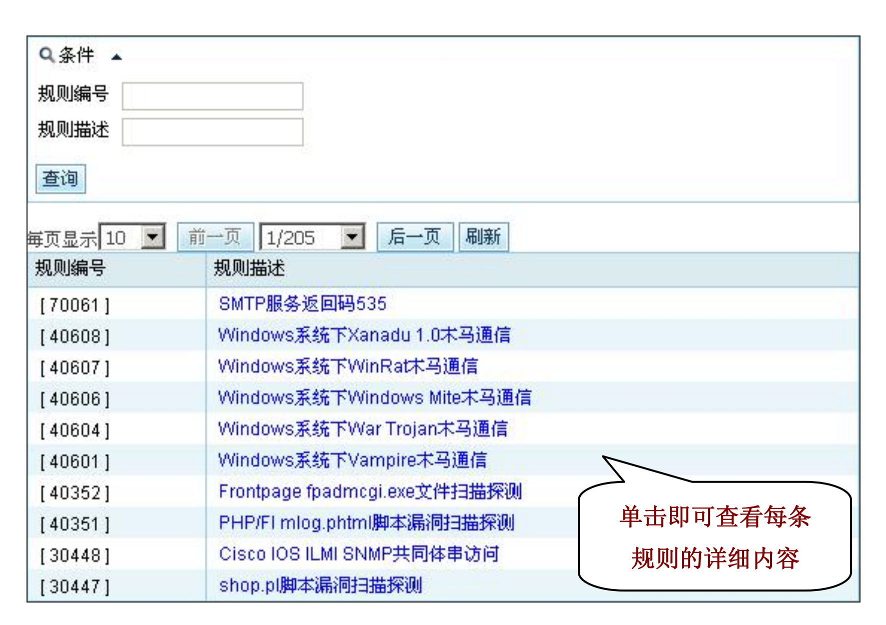


图 11.1 帮助 – 规则库搜索

下面分别介绍两种搜索规则的方法：

◆ **按规则编号**

每条规则都有自己的编号，可以直接指定规则号进行搜索。例如：输入 *10000*，单击【查询】后，在查询结果列表中列出规则号中所有包含 *10000* 的规则。

◆ **按规则描述**

按照规则描述进行搜索。例如：输入*远程登录*，单击【查询】后，在查询结果列表中列出规则信息中所有包含*远程登录*的规则。

系统支持通过引擎升级方式更新帮助信息。

附录A 出厂参数

A.1 引擎管理口初始设置

IP	eth0:192.168.1.1 eth1:192.168.2.1 eth2:192.168.3.1 eth3:192.168.4.1 ……（若有更多网口，初始 IP 依此类推）
网络掩码	255.255.255.0

A.2 引擎初始用户

A.2.1 Web 操作员初始帐号

<table><tr><td>用户名</td><td rowspan="2">weboper</td></tr><tr><td>密　码</td></tr></table>

A.2.2 Web 审计员初始帐号

<table><tr><td>用户名</td><td rowspan="2">webaudit</td></tr><tr><td>密　码</td></tr></table>

A.2.3 串口管理员初始帐号

<table><tr><td>用户名</td><td rowspan="2">conadmin</td></tr><tr><td>密　码</td></tr></table>

A.3 绿盟安全中心管理员初始帐号

<table><tr><td>用户名</td><td rowspan="2">admin</td></tr><tr><td>密　码</td></tr></table>

A.4 串口通讯参数

波 特 率	115200
传输位数	8

A.5 CLI 管理员初始帐号

用户名	shell
密　码	